논문 2023-2-3 http://dx.doi.org/10.29056/jsav.2023.06.03

디지털 콘텐츠 저작권료 정산 및 분배를 위한 블록체인 기반 원화 이체 시스템 설계

최창준*, 조용준*, 신동명*†

Design of a Blockchain-based KRW Transfer System for Settlement and Distribution of Digital Content Copyright Fees

Chang-Jun Choi*, YongJoon Joe*, Dong-Myung Shin*†

요 약

최근 디지털 콘텐츠 산업의 성장으로 창작물에 대한 복잡한 권리관계가 형성되고, 이로 인해 공정하지 못한 저작권료 정산 문제가 발생하고 있다. 이를 해결하기 위해 블록체인 기술을 활용한 연구가 다양하게 진행되고 있지만, 외부 시스템과 능동적으로 연동될 수 없는 기존 블록체인 시스템의 기술적인 제약으로 인해 저작권료 이체 요청에 따른 외부 데이터에 대한 신뢰성을 보장할 수 없다는 한계점이 있다. 이에 따라, 본 논문에서는 블록체인과 외부 시스템 간 상호작용 과정에서 이체 트랜잭션을 스케줄링하여 이체 요청에 의한 외부 시스템의 중복 실행을 방지하고, 각 참여 노드들이 외부 입출력 정보를 상호검증하여 외부 데이터의 신뢰성을 보장할 수 있는 원화 이체 시스템을 제안하고자 한다. 제안된 시스템에서는 단일 트랜잭션 내에서 블록체인 요청 처리를 완결시키므로 처리 성능과 응답 속도를 향상시키며, 합의에 참여하는 모든 노드에게 외부 실행 결과가 전파되어 외부 데이터의 일관성과 신뢰성을 보장한다.

Abstract

Recently, the growth of the digital content industry has led to complex rights relationships for creative works, resulting in unfair issues with copyright royalty settlements. To address these problems, various research efforts have been conducted using blockchain technology. However, the existing blockchain systems have limitations in actively integrating with external systems, making it difficult to guarantee the reliability of external data related to copyright royalty transfers. Therefore, this paper proposes a fiat currency transfer system that ensures the reliability of external data by scheduling transfer transactions and preventing duplicate execution of external systems, as well as enabling mutual verification of input/output information among participating nodes during the interaction process between blockchain and external systems. The proposed system improves performance and response speed by completing blockchain requests within a single transaction and ensures the consistency and reliability of external data by propagating the results to all participating nodes.

한글키워드 : 디지털 콘텐츠, 블록체인, 저작권료, 원화 이체, 정산·분배

keywords : Digital Contents, Blockchain, Copyright Fees, KRW Transfer, Settlement/Distribution

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

접수일자: 2023.05.31. 심사완료: 2023.06.14.
게재확정: 2023.06.20.

1. 서 론

최근 1인 미디어의 활성화 및 디지털 콘텐츠의 수요가 급증함에 따라 콘텐츠를 제작하고 유통 및 관리하는 형태가 다양해지고 있다. 반면에, 디지털 콘텐츠의 생산과 소비가 증가함에 따라 저작권 침해와 분쟁의 가능성도 증가하고 있으며, 기존 실물 콘텐츠와 동일한 오프라인 정산 방식이 적용되고 있어, 디지털 콘텐츠 창작자들의 권리 보호가 어려워지고 있다[1]. 또한, 디지털 콘텐츠는 온라인상에서 쉽게 수정, 재사용 및 재배포될 수 있기 때문에 이용허락이 빈번하게 발생하며, 다양한 플랫폼과 서비스를 통해 불특정 다수에게 유통되므로 콘텐츠 이용허락과 관련된 라이선스 정보 추적 관리에 어려움을 겪고 있는 실정이다.

이러한 문제를 해결하기 위해 최근에는 블록체인 기술을 활용하여 디지털 콘텐츠에 대한 권리 및 이용허락 정보를 투명하게 기록하고 추적할 수 있는 연구가 진행되고 있다[2]. 블록체인은 제3의 신뢰 기관 없이 네트워크 참여 노드 간 콘텐츠의 이용허락 정보 등을 분산원장에 기록하여 데이터의 투명성과 무결성을 보장할 수 있는 기술이다. 그러나 저작권료 정산과 같이 은행 결제 과정을 처리하기 위해서는 외부 시스템과 연동이 요구되며 이 과정에서 이종 시스템 간 상호운용성 문제 및 오라클 문제로 인한 블록체인 데이터의 신뢰성을 저하시키는 문제가 발생할 수 있다.

따라서, 본 논문에서는 블록체인 환경에서 디지털 콘텐츠에 대한 저작권료 정산 시 상호운용성을 위해 표준화된 데이터 형식을 제공하여 블록체인 노드 및 외부 시스템 간 입출력 정보를 상호 검증할 수 있는 원화 이체 시스템을 제안한다. 제안하는 시스템에서는 프록시(Proxy) 서버를 통해 스마트 컨트랙트에서의 외부 데이터 활용을 용이하게 함으로써, 저작권료 정산에 필요한 이체 트랜잭션의 신뢰성을 보장한다.

2. 관련 연구

2.1 기존 콘텐츠 저작권료 정산 방식의 문제점

디지털 콘텐츠 산업은 급속도로 성장하고 있으며, 이에 따라 콘텐츠 창작자들의 수도 증가하고 있다. 디지털 콘텐츠는 여러 창작자에 의해 N차적으로 수정, 보완, 가공되어 창작되는 경우가 많으므로, 여러 이해관계자 간에 복잡한 저작권 권리관계가 형성된다. 이에 따라, 디지털 콘텐츠가 유통될 때에는 창작자와 이용자 간 계약 내용을 명확히 정해야 하며, 이용된 콘텐츠에 대한 정산 데이터를 투명하게 공개하여 정확하고 신뢰성 있는 저작권료 정산이 이루어져야 한다.

하지만 기존 불투명한 오프라인 정산 방식, 또는 정산 내역의 비공개로 인하여 저작권료를 공정하게 정산받지 못하는 문제가 빈번하게 발생하고 있다. 일반적인 콘텐츠 유통업체에서는 실제로 발생한 저작권료의 정산액이나 저작물의 이용현황 등을 공개하는 경우가 드물며, 대부분 표준계약서 혹은 서비스 이용약관 등을 통해 저작권료 정산에 관한 규정만을 명시하고 있다[3]. 이로 인해 창작자들은 자신의 창작물이 어떻게 이용되고 있는지, 콘텐츠에서 발생한 저작권료가 얼마인지 정확하게 파악할 수 없어 객관적인 정산이나 권리 요구를 보장받지 못하는 결과를 가져오고 있다.

또한, 기존 저작권료 정산 방식은 디지털 콘텐츠의 사용 범위나 기간 등을 고려하지 않고, 단순히 조회수나 판매량 등을 기준으로 지급하기 때문에 저작권자가 적절한 보상을 받지 못할 가능성이 있다[4]. 이러한 방식은 저작권자들의 이익을 침해할 뿐만 아니라, 콘텐츠 창작 의욕을 저하시켜 결과적으로 디지털 콘텐츠 산업의 지속

적인 성장을 방해할 가능성도 있다. 따라서, 이러한 문제점을 해결하기 위해서는 저작권자의 권리를 보호할 수 있는 체계적인 시스템을 구축하고 이를 통해 공정하고 투명하게 저작권료를 정산할 수 있는 기술적인 개선 방안이 필요한 실정이다.

2.2 블록체인 오라클 문제

블록체인은 분산원장 기술을 활용하여 데이터의 투명성과 신뢰성을 보장하는 기술이다. 이는 P2P (Peer-to-Peer) 기반 분산된 네트워크 환경에서 모든 참여 노드들이 공동으로 데이터를 검증하며, 검증된 데이터를 블록에 추가함으로써 제3의 신뢰 기관 없이 데이터의 신뢰성을 확보한다. 그러나, 블록체인 내부에서 특정 조건이 충족되면 자동으로 실행되는 스마트 컨트랙트의 특성상 블록체인 외부(off-chain) 시스템 자체에 대한 직접적인 접근은 불가능하므로, 외부 시스템의 데이터에 대해서는 신뢰성을 보장하기 어렵다. 블록체인에서는 이러한 기술적인 한계를 보완하기 위해, 외부 데이터를 수집하고 이를 블록체인 내부로 전달하는 오라클(Oracle)을 활용하여 외부 시스템과의 상호작용을 가능하게 한다.

오라클을 통해 외부 시스템과 연동이 가능해지면서 블록체인 시스템의 활용 범위가 확대되었지만, 오라클이 제공하는 외부 데이터에 대한 조작 가능성과 검증의 부재로 인해 데이터 정확성이 보장되지 않는 신뢰성 문제는 여전히 발생하고 있다[5]. 블록체인과 같은 분산된 네트워크 환경에서는 노드 간 통신 지연 및 네트워크 상황에 따라 스마트 컨트랙트의 실행 시간이 서로 다를 수 있으므로, 오라클을 통해 외부 시스템으로 명령을 내리거나 외부 데이터를 블록체인 내부로 가져올 때, 데이터를 상호 검증하는 각 노드의 트랜잭션 실행 결과가 달라질 가능성이 있다. 이로 인해 각 블록체인 참여 노드들이 데이터 검증에 실패하여 결과적으로 블록체인 시스템의 고유 특성인 신뢰성이 보장되지 않는 문제가 발생할 수 있다. 이러한 블록체인 오라클 문제를 해결하기 위해서는 외부 데이터의 활용과 검증에 대한 기술적인 개선이 필요하며, 각 노드의 트랜잭션 실행 결과를 일관성 있게 유지시킬 수 있는 효율적인 외부 상호작용 방법이 요구된다.

3. 원화 이체 시스템 설계

본 장에서는 제안하는 시스템의 고려사항을 분석하고 전체적인 원화 이체 동작 프로세스를 설명한다.

3.1 시스템 고려사항 분석

블록체인과 같은 분산 시스템에서는 네트워크 지연, 하드웨어 성능 차이 등과 같은 요인으로 인해 노드 간의 정확한 시간 동기화가 어렵다[6]. 이러한 시간 동기화의 어려움으로 인해 분산 시스템에서는 데이터의 일관성이 유지되지 않는 문제가 발생할 수 있다. 분산된 네트워크 환경에서 데이터의 신뢰성을 보장하는 블록체인에서는 노드 간에 일관된 원장 상태를 유지하기 위해 합의 알고리즘을 이용하여 분산 노드의 동기화 문제를 해결한다. 하지만, 대부분의 합의 알고리즘은 블록 생성 및 체인 유지에 초점을 맞추고 있으며, 트랜잭션 검증 과정에 대한 보안성은 주로 합의 메커니즘의 내부적인 수학적 모델링 증명에만 집중되어 있다[7].

블록체인에서의 외부 데이터 활용은 스마트 컨트랙트와 외부 시스템 간 상호작용을 포함한다. 스마트 컨트랙트의 상태 변화에 따라 외부 시스템에서 업데이트가 필요한 경우, 외부 시스템의 응답이 지연되거나 오류가 발생할 수 있다. 따라서, 스마트 컨트랙트에서 이미 처리된 외부 데이터에 대해 추가적인 동작을 수행하지 않도록

해야 하며, 블록체인과 외부 시스템을 연결해주는 미들웨어 레벨에서 적절한 로직과 메커니즘을 적용하여 데이터 일관성 유지 및 중복 실행 문제를 동시에 해결할 수 있도록 해야 한다.

또한, 스마트 컨트랙트를 이용한 저작권료 정산을 위해서는 사용자의 개인 정보(e.g., 영업 비밀 계약 정보 등)가 원장에 기록될 수 있기 때문에 정산에 필요한 개인 식별이 가능한 정보는 익명화하거나 암호화하여 관리되어야 하고, 허가된 블록체인 노드만이 접근할 수 있도록 권한을 제어하여 개인 정보 노출을 최소화해야 한다[8][9].

3.2 시스템 구조 및 동작과정

본 논문에서 제안하는 시스템은 디지털 콘텐츠에 대한 저작권료 정산을 위해 전자지급결제대행(PG, Payment Gateway) 서비스를 활용한다. PG 서비스는 온라인 전자상거래에서 플랫폼(가맹점)과 사용자 간 안전한 결제수단을 제공하는 중개 역할을 수행한다[10]. 제안 시스템에서는 프록시 서버에서 PG 서비스의 전자결제 API를 호출하며, 비밀 공유 기법(Secret Sharing Scheme)을 통해 각 블록체인 노드에서 호출되는 스마트 컨트랙트의 이체 요청을 스케줄링한다. 비밀 공유 기법은 여러 개체 또는 그룹의 구성원 간에 안전하게 정보를 공유하기 위해 사용되며, 하나의 비밀 정보(Secret)를 여러 개의 비밀 조각(Share)으로 분할하고, 일정 수(threshold) 이상의 비밀 조각이 모이면 비밀 정보를 복원할 수 있는 방식이다[11]. 이를 통해 다수의 구성원이 합의를 이루어 특정 정보를 확인하거나 제공해야 하는 상황에서 데이터의 기밀성과 무결성을 보장한다[12].

제안하는 원화 이체 시스템에서는 스마트 컨트랙트의 요청에 따른 PG API 중복 실행을 제어하기 위해, 각 블록체인 노드의 비밀 조각(이체 트랜잭션)을 일정 수만큼 수신한 경우에만 PG API를 호출할 수 있게 한다. 전체적인 시스템 구조는 그림 1과 같으며, 저작권료 정산을 위해 다음과 같은 과정을 수행한다.

① **세션 유지**: 각 블록체인 참여 노드들은 프록시 서버와의 통신을 위해 세션을 수립(요청)한다. 이후 노드 간 합의를 통해 비밀 정보 복원에 필요한 최소 비밀 조각의 개수를 결정하여 프록시 서버에 전달한다.

② **API 요청 대기**: 블록체인에서 이체 트랜잭션 발생 시, 각 노드들은 PG API 호출에 필요한 정보를 페이로드(Payload)로 형태로 생성하고, 이를 비밀 조각으로 활용하여 프록시 서버로 전달한다. 프록시 서버에서는 일정 수 이상의 페이로드를 수신하기 전까지 각 블록체인 노드가 요청한 내용을 알 수 없으므로, 충분한 수 만큼의 비밀 조각(페이

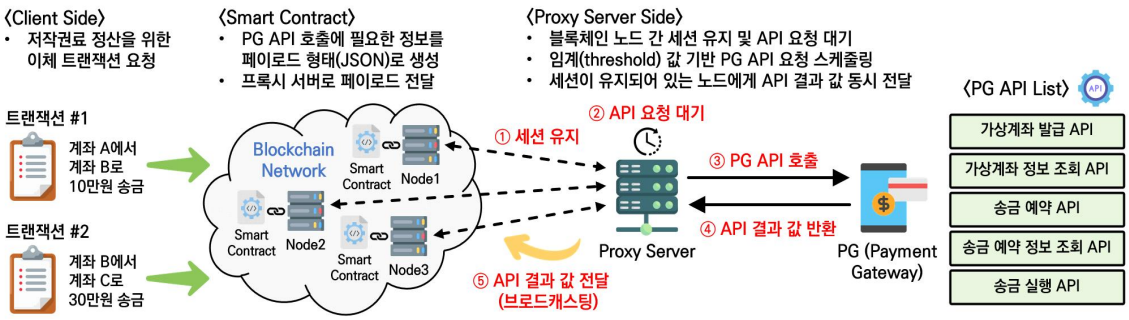


그림 1. 원화 이체를 위한 PG API 호출 프로세스
Fig. 1. PG API Calling Process for KRW Transfer

로드)을 수신할 때까지 대기한다.

③ **PG API 호출**: 합의된 비밀 조각 개수만큼 페이로드를 수신한 경우, 프록시 서버는 이를 API 호출 형식으로 변환하여 페이로드에서 요청하는 PG API를 호출한다.

④ **API 결과 값 반환**: PG 서버는 프록시 서버에서 요청한 PG API를 실행하고, 이에 대한 결과 값을 프록시 서버로 반환한다.

⑤ **API 결과 값 전달**: 프록시 서버는 세션이 유지되어 있는 모든 노드에게 PG API 실행 결과를 동시에 반환한다. 각 노드들은 이체 트랜잭션의 실행 결과를 상호 검증하여 합의를 수행하고, 그 결과를 블록체인 원장에 기록한다.

3.2.1 페이로드 생성 및 외부 API 호출

스마트 컨트랙트에서 외부 기능(e.g., PG API)을 실행할 때는 그림 2와 같이 이체에 필요한 정보를 JSON 형태의 페이로드로 패키징하고, 이를 비밀 조각으로 활용하여 프록시 서버로 전달한다. 페이로드 내부에는 프록시 서버가 이체 트랜잭션을 구별하기 위한 레퍼런스 ID(ref_id), 프록시 서버에서 호출할 PG API 주소(api_path), 스마트 컨트랙트에서 이체 성공 여부를 구별하기 위한 ID(guid), 그리고 PG 가상계좌 생성 및 송금 예약/실행에 사용되는 요청 정보(req_body)가 포함된다.


```
{
  "ref_id":"REFID#e55db88d7e62ae8",
  "api_path":"account",
  "guid":0,
  "req_body":{
       "transaction_id":"e55db88d7e62ae8",
       "account_id":"gildong123_e1b8c4165c67fa28e6",
       "owner":"gildong123",
       "balance":1000000,
       "held":0
   }
}
```


그림 2. 페이로드 예시 (가상계좌 발급)
Fig. 2. Payload Example (Virtual Account Issuance)

프록시 서버에서의 PG API 호출은 표 1과 같이 HTTP 메서드를 통해 실행된다. 각 PG API에 대한 설명은 다음과 같다.

표 1. PG API 리스트 및 호출 메서드
Table 1. PG API Lists and Call Methods

#	PG API	API Path (HTTP Method)
1	가상계좌 발급	**POST** "http://<PG_URL>/account"
2	가상계좌 정보 조회	**GET** "http://<PG_URL>/account/{account_id}"
3	송금 예약 (Holding)	**POST** "http://<PG_URL>/holding"
4	송금 예약 정보 조회	**GET** "http://<PG_URL>/holding/{transaction_id}"
5	송금 실행 (Release)	**POST** "http://<PG_URL>/hold/release/id/{ExternalID}"

(1) **가상계좌 발급**: 가상계좌 발급 API는 페이로드에 포함된 사용자 정보를 기반으로 PG 가상계좌를 할당하는 기능을 제공한다. 이를 통해 발급되는 계좌는 실제 은행 계좌가 아니며, 결제를 위한 임시 계좌로 사용된다.

(2) **가상계좌 정보 조회**: 가상계좌 정보 조회 API는 사용자의 가상계좌 ID(account_id)를 이용하여 PG 서버에서 관리하는 가상계좌의 상태 정보(e.g., 사용자 ID 및 계좌 잔액 등)를 조회하는 기능을 제공한다.

(3) **송금 예약(Holding)**: 송금 예약 API는 페이로드에 포함된 사용자의 가상계좌 ID 및 이체 금액 등을 통해 송금할 금액을 예약 상태로 설정하는 기능을 제공한다. 실제로 송금이 이루어지기 전에 이체를 보류시키고 가상계좌의 잔액 및 이체 가능 여부를 확인할 수 있다.

(4) **송금 예약 정보 조회**: 송금 예약 정보 조회 API는 송금 예약 시 활용된 트랜잭션 ID를 통해 가상계좌의 예약된 송금 내역을 조회하는 기능을 제공한다. 반환되는 정보에는 PG 서버 내부적으로 송금 처리를 관리하기 위한 External ID가 포함되어 있다. External ID

는 송금 실행(Release) API에서 예약 내역에 대한 최종 이체를 수행할 때 사용된다.

(5) **송금 실행(Release)**: 송금 실행 API는 PG 서버에서 관리하는 External ID를 입력으로 받아 보류 중인 송금액을 최종적으로 수취인의 가상계좌에 이체하는 기능을 제공한다. API 실행 결과로 송금이 정상적으로 처리되었는지 여부를 반환한다.

대부분의 PG 서비스는 REST API 방식을 통해 전자결제에 필요한 기능을 제공하고 있기 때문에 프록시 서버는 HTTP 프로토콜을 이용하여 PG 서버와 상호작용한다. 제안 시스템에서의 PG API 호출에 대한 세부 프로세스는 다음과 같다.

3.2.2 PG 가상계좌 발급 프로세스

스마트 컨트랙트에서는 발급받을 가상계좌 정보를 페이로드 형태로 변환한 후, 프록시 서버로 전송한다. 프록시 서버는 동일한 트랜잭션 요청이 담긴 페이로드를 임계값(세션이 연결된 블록체인 노드 수)만큼 수신할 때까지 대기하며, 각 페이로드의 요청 내용이 동일한지 확인한다. 이후 PG API 호출 형태로 변환하여 PG 가상계좌 발급을 호출한다. PG 서버에서는 프록시 서버로부터 수신한 페이로드를 기반으로 가상계좌 발급 API를 실행한다. 프록시 서버는 가상계좌 발급 API의 실행 결과(발급 성공/실패 메시지)를 세션이 연결된 각 노드의 스마트 컨트랙트로 동시에 반환한다.

3.2.3 PG 가상계좌 정보 조회 프로세스

스마트 컨트랙트에서는 블록체인 원장에 기록되어 있는 사용자의 가상계좌 정보(e.g., 은행명, 예금주명, 계좌번호 등)를 식별하기 위한 가상계좌 ID(account_id)를 생성한다. 이후, 스마트 컨트랙트에서 직접 PG API를 호출한다. PG 서버에서는 수신한 가상계좌 ID를 기반으로 PG에서 관리하는 사용자의 가상계좌 정보를 조회하며, API 실행 결과를 스마트 컨트랙트로 반환한다.

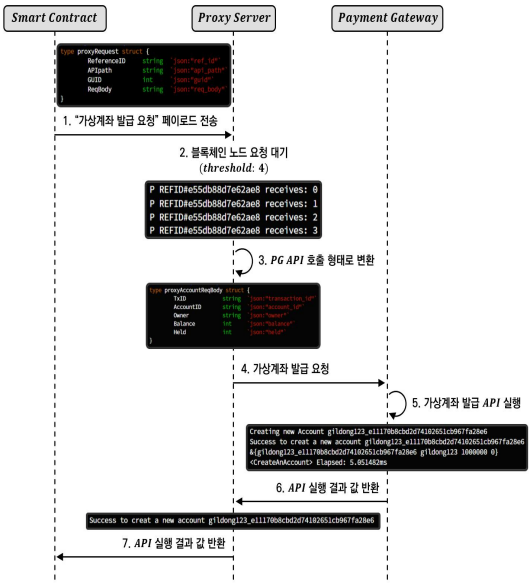


그림 3. PG 가상계좌 발급 시퀀스
Fig. 3. PG Virtual Account Issuance Sequence

그림 4. PG 가상계좌 정보 조회 시퀀스
Fig. 4. PG Virtual Account Query Sequence

3.2.4 송금 예약(Holding) 프로세스

스마트 컨트랙트에서는 블록체인 원장에 기록되어 있는 송금인(Sender) 및 수취인(Receiver)의 가상계좌를 조회하여 Holding 페이로드를 생성한다. 생성된 페이로드는 프록시 서버로 전송되며, 프록시 서버에서는 동일한 트랜잭션 요청이 담긴 페이로드를 임계값만큼 수신할 때까지 대기한다. 이후, 프록시 서버는 송금인의 가상계좌에서 송금액(HoldAmount)을 예약 상태로 설정하기 위해 페이로드 정보를 PG API 호출 형태로 변환 후, PG 서버에 API 실행을 요청한다. PG 서버는 API 실행 결과인 성공/실패 메시지를 프록시 서버로 반환하며, 프록시 서버에서는 세션이 연결된 각 블록체인 노드에게 해당 결과를 반환한다.

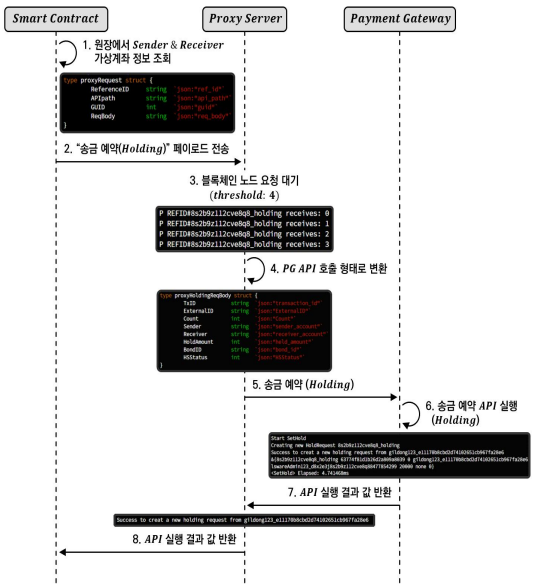


그림 5. 송금 예약(Holding) 시퀀스
Fig. 5. Transfer Holding Sequence

3.2.5 송금 실행(Release) 프로세스

스마트 컨트랙트에서는 송금 예약 시 사용된 트랜잭션 ID를 통해 해당 ID와 매핑되는 송금 예약 정보를 조회한다. PG 서버는 트랜잭션 ID를 기반으로 송금 예약 정보와 함께 송금 처리를 위한 PG 서버의 관리용 식별자인 External ID를 반환한다. 스마트 컨트랙트에서는 Release 페이로드에 External ID를 포함시켜 프록시 서버로 전송한다. Release 페이로드에는 송금인/수취인의 가상계좌 정보 및 송금액, External ID 등 실제 이체에 필요한 정보가 포함된다. 프록시 서버는 모든 블록체인 요청을 수신할 때까지 대기하며, 요청이 완료되면 Release 페이로드를 PG API 호출 형태로 변환하여 송금 실행 API를 호출한다. PG 서버에서는 송금인의 가상계좌에 예약되어있는 송금액을 확인하고, 최종적으로 이체 처리를 수행한다. PG 서버의 API 실행 결과에는 최종 이체 처리 정보가 포함되며, 프록시 서버를 통해 각 노드들에게 반환된다.

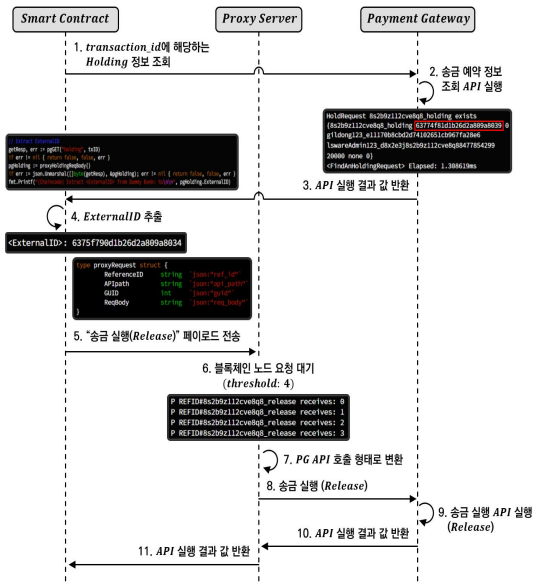


그림 6. 송금 실행(Release) 시퀀스
Fig. 6. Transfer Release Sequence

제안하는 시스템에서는 디지털 콘텐츠 이용에 따라 발생하는 저작권료를 예약 상태로 설정하여 이용자의 가상계좌에서 다른 용도로 사용되지 않

도록 할당한다. 각 블록체인 노드의 스마트 컨트랙트에서는 저작권료를 정산하기 위한 트랜잭션이 발생했을 때, PG 서버의 송금 실행 API를 활용하여 예약된 저작권료에 대한 정산을 수행한다. 정산 이벤트 발생 시, PG 서버는 해당 이용자의 가상계좌에서 저작권료 정산액을 적절한 수령자에게 송금하는 절차를 진행한다. 스마트 컨트랙트와 PG 서버 간 상호작용을 위해 미들웨어 역할을 수행하는 프록시 서버는 블록체인 노드들이 외부 시스템의 API 실행 결과를 상호 검증할 수 있도록 하며, 저작권료 정산 처리를 단일 트랜잭션 내에서 수행할 수 있도록 한다. 이를 통해 디지털 콘텐츠 이용에 따른 저작권료의 정확한 정산과 분배를 보장하며, 블록체인을 통한 정산 과정의 전체적인 효율성을 향상시킨다.

4. 제안 시스템 평가 및 분석

본 논문에서는 저작권료 정산을 위해 블록체인과 외부 시스템 간 연동 시, 단일 트랜잭션 요청에 대한 외부 시스템의 중복 실행 문제 및 블록체인 외부 데이터의 상호 검증 문제를 해결하기 위한 시스템을 제안한다. 기존 오라클 방식은 이러한 문제를 해결하기 위해 복수 서명 시스템을 도입하고 있었으나, 이는 합의에 참여하는 각 블록체인 노드의 서명이 트랜잭션에 포함되어 모두 확정될 때까지 대기해야 하므로, 외부 요청 처리에 대한 응답 지연 문제를 발생시킨다. 또한, 외부 API 요청이 요구되는 트랜잭션이 블록에 포함되어 확정될 경우, 해당 블록을 확인하기 위해 오라클 노드에서 서명(보고) 트랜잭션을 생성하고, 블록체인에서는 외부 요청이 완료된 이후의 사후 처리를 위한 트랜잭션이 다시 수행되기 때문에 시스템 처리 성능 면에서 불필요한 오버헤드를 발생시킨다. 이러한 방식은 전체 시스템 효율성과 응답성을 저하시켜 저작권료 정산 처리의 정확성과 완결성을 보장할 수 없게 된다.

따라서, 본 논문에서는 블록체인과 외부 시스템 간의 상호작용 과정에서 스마트 컨트랙트의 요청을 효율적으로 처리하기 위한 메커니즘을 제안하였다. 제안 시스템에서는 블록체인 요청 처리가 단일 트랜잭션 내에서 완결되므로, 처리 성능 및 응답 속도를 향상시킨다. 외부 시스템의 응답에 대한 검증의 경우 블록체인 내부에서 이루어지며, 특히 외부 실행 결과는 서로 다른 기관에 속하는 모든 노드의 합의를 통해 외부 데이터의 일관성과 신뢰성을 확보할 수 있다[13]. 다만, 이러한 방식은 기존 PoS (Proof-of-Stake) 및 PoW (Proof-of-Work)와 같은 리더 노드 선출 방식 또는 블록 생성 경쟁 방식에서 채택하기 어려운 방식이라는 점에서 확장성을 개선하기 위한 접근 방법을 추가로 고려해야 한다.

5. 결 론

블록체인은 분산원장 기술을 활용하여 데이터의 투명성과 신뢰성을 보장하는 기술이다. 그러나 스마트 컨트랙트의 특성상 블록체인 외부 시스템에 직접적인 접근이 불가능하고, 외부 데이터의 신뢰성을 보장하기 어려운 한계가 존재한다. 이를 보완하기 위해 기존 시스템에서는 오라클을 활용하여 외부 상호작용을 가능하게 하였지만, 외부 데이터에 대한 검증의 부재로 인해 신뢰성 문제가 여전히 발생하고 있다. 이러한 신뢰성 문제는 디지털 콘텐츠에 대한 저작권료 정산 시 매우 치명적인 문제로 작용할 수 있다. 정확하고 신뢰할 수 있는 저작권료 정산 과정은 창작자와 이용자 간의 공정한 보상 체계를 구축하기 위한 핵심 요소이며, 창작자의 권익 보호를 위해 매우 중요하다.

이에 따라, 본 논문에서는 디지털 콘텐츠의 저작권료 정산 과정에서 발생할 수 있는 외부 데이터의 조작 가능성과 검증 부재 문제를 해결할 수 있는 블록체인 기반 원화 이체 시스템을 제안하였다. 제안된 방식에서는 프록시 서버가 중간자 역할을 수행하며, 블록체인에서 발생한 이체 트랜잭션의 중복 실행을 방지하기 위해 비밀 공유 기법을 활용한다. 프록시 서버는 각 참여 노드의 스마트 컨트랙트와 외부 시스템(PG 서버) 간 블록체인 요청을 스케줄링하여 PG API 호출을 제어한다. 이를 통해 블록체인 외부로 특정 명령어를 전달하는 과정에서 스마트 컨트랙트 및 외부 시스템 간 송수신되는 데이터의 신뢰성을 보장한다.

본 연구는 문화체육관광부 및
한국콘텐츠진흥원의 2023년도 가상공연 핵심 기술개발 사업으로 수행되었음 (과제명 : 대규모 가상공연 플랫폼을 지원하는 블록체인 기반 저작물 보호 및 활용 기술 개발, 과제번호 : R2022020057, 기여율 : 100%)

참 고 문 헌

[1] H. Sim, “A Study on Digital Content Copyright Management and Verification Platform using Blockchain”, The Journal of the Korea institute of electronic communication sciences, vol. 17, no. 1, pp. 193 - 200, (Feb. 2022). DOI: 10.13067/JKIECS.2022.17.1.193

[2] Y.-M. Kim, B.-C. Park, K.-S. Bang, and S.-Y. Kim, “A Method of Generating Theme, Background and Signal Music Usage Monitoring Information Based on Blockchain”, Journal of the Korea Society of Computer and Information, vol. 26, no. 2, pp. 45 - 52, (Feb. 2021). DOI: 10.9708/JKSCI.2021.26.02.045

[3] H. W. Nam, “A Study on the Copyright Calculation, Settlement, Monitoring, and Blockchain Framework for Art Contents”, Korea Institute of Design Research Society, vol. 6, no. 1. Korea Institute of Design Research Society, pp. 146 - 157, (Mar. 2021). DOI: 10.46248/kidrs.2021.1.146

[4] J.-Y. Lee, D.-K. Sung, and J.-S. Lee, “A study on the Development of Digital Music Industry in Korea”, Journal of Digital Contents Society, vol. 21, no. 11. Digital Contents Society, pp. 1981 - 1989, (Nov. 2020). DOI: 10.9728/dcs.2020.21.11.1981

[5] G. Caldarelli, “Understanding the Blockchain Oracle Problem: A Call for Action”, Information, vol. 11, no. 11. MDPI AG, p. 509, (29-Oct-2020). DOI: 10.3390/info11110509

[6] Distefano, S., & Puliafito, A. Information dependability in distributed systems: The dependable distributed storage system. Integrated Computer- Aided Engineering, 21(1), 3-18, (2014). DOI: 10.3233/ICA-130444

[7] S. Lee, B. Lee, S. Myung, and J.-H. Lee, “Security Analysis of Blockchain Systems: Case Study of Cryptocurrencies”, Journal of the Korea Institute of Information Security & Cryptology, vol. 28, no. 1, pp. 5 - 14, (Feb. 2018). DOI: 10.13089/JKIISC.2018.28.1.5

[8] Y.-H. Kim, “A Study on Smart Contract for Personal Information Protection”, Journal of Digital Convergence, vol. 17, no. 3, pp. 215 - 220, (Mar. 2019). DOI: 10.14400/JDC.2019.17.3.215

[9] J.-S. Park and S. U. Shin, “Analysis of Blockchain Platforms from the Viewpoint of Privacy Protection”, Journal of Internet Computing and Services, vol. 20, no. 6, pp. 105 - 117, (Dec. 2019). DOI:

10.7472/JKSII.2019.20.6.105
[10] Lee, Jieun, Heo, Jeongyun, and Hochang Kwon, “User Experience Study on Online Payment Services - Focusing on Payment Gateway(PG) Services”, Journal of Payment and Settlement, vol. 14, no. 2, pp. 271 - 302, (Dec. 2022). DOI: 10.22898/KPSAKR.2022.14.2.271
[11] E. Karnin, J. Greene, and M. Hellman, “On secret sharing systems”, IEEE Transactions on Information Theory, vol. 29, no. 1. Institute of Electrical and Electronics Engineers (IEEE), pp. 35 - 41, (Jan. 1983). DOI: 10.1109/tit.1983.1056621
[12] A.-S. Son, S.-B. Yoo, J.-H. Jo, and S.-M. Yoo, “A Study on Smart Contract Platform using Secret Sharing Scheme”, The Journal of Korean Institute of Information Technology, vol. 18, no. 11. Korean Institute of Information Technology, pp. 131 - 138, (30-Nov-2020). DOI: 10.14801/jkiit.2020.18.11.131
[13] Yang, G., Lee, K., Lee, K., Yoo, Y., Lee, H., & Yoo, C. “Resource Analysis of Blockchain Consensus Algorithms in Hyperledger Fabric”, IEEE Access, 10, 74902-74920. (14-Jul-2023). DOI: 10.1109/ACCESS.2022.319097

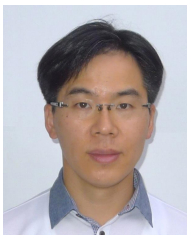
저 자 소 개

최창준(Chang-Jun Choi)

2019.2 상명대학교 컴퓨터공학과 졸업
2021.8 세종대학교 정보보호학과 석사
2021.9-현재 엘에스웨어㈜ 주임연구원
<주관심분야> 정보보호, 네트워크 보안, 블록체인, 분산신원인증

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㈜ 연구소장/상무이사
<주관심분야> 오픈소스 라이선스, 저작권 기술, 시스템/네트워크 보안, SW취약점 분석·감정, 블록체인 기술