

블록체인 기반 오프체인 동영상 스트리밍 시스템

*정민혁 **김상균

명지대학교

**goldmunt@gmail.com

Off-chain Video Streaming System based on Blockchain

*Jeong, Min-Hyuk **Kim, Sang-Kyun

Myongji University

요약

블록체인의 특성 중 하나인 합의 과정으로 인해 블록체인 상 거래속도는 일반적인 온라인 거래보다 느리다는 단점이 있다. 분산형 어플리케이션 서비스들은 이러한 블록체인의 느린 거래속도와 확장성을 오프체인 트랜잭션으로 해결한다. 오프체인 트랜잭션이란 블록체인 외부에서 거래를 실행하여 이루어진 거래들의 내역을 주기적으로 블록체인에 기록하는 방식이다. 오프체인 트랜잭션을 활용하면 기존의 블록체인 거래방식보다 더 다양한 구조로 시스템을 설계할 수 있다. 본 논문에서는 이러한 오프체인 트랜잭션의 장점을 활용한 실시간 비디오 스트리밍 시스템을 제안한다. 사용자와 서비스 제공자 간의 거래를 위한 오프체인 채널을 연 후 채널 상에서 실시간으로 비용을 지불하고 비디오를 스트리밍 받는 시스템을 설계하였다. 이러한 실시간 스트리밍 방식을 통해 기존 블록체인 서비스의 단점을 극복하였다.

1. 서론

블록체인을 통해 거래를 할 때 노드 간에 일어나는 합의 과정으로 인해 즉각적인 거래를 할 수 없다. 또한 거래가 발생할 때 마다 수수료가 발생한다. 따라서 블록체인 기반 서비스들은 거래 횟수를 최소한으로 하는 구조를 택한다. 이러한 구조적 제한은 블록체인 서비스를 다양하게 설계할 수 없도록 한다[1].

블록체인 서비스들은 이러한 구조적 한계를 오프체인 트랜잭션으로 극복하려고 한다. 오프체인 트랜잭션은 메인 블록체인 밖에서 거래를 하는 시스템이다. 블록체인 밖에서 거래를 진행하여 메인 블록체인의 처리량 부담을 덜고 빠른 거래를 할 수 있는 장점이 있다. 오프체인의 종류에는 오프체인이 일반적인 컴퓨터 통신으로 구성된 상태 채널 트랜잭션과 오프체인이 또 다른 블록체인으로 구성된 사이드체인, 차일드체인이 있다[2].

본 논문에서는 오프체인 트랜잭션 중 상태 채널을 이용한 비디오 스트리밍 시스템을 제안한다. 상태 채널을 통하여 실시간으로 비용을 지불하고 비디오를 스트리밍 받는 시스템을 설계하였다.

논문의 구성은 다음과 같다. 2장에서는 오프체인 비디오 스트리밍 시스템의 개요와 구조에 대해 설명한다. 3장에서는 향후 연구 과제에 대해 도출한다.

2. 오프체인 비디오 스트리밍 시스템

오프체인 비디오 스트리밍 시스템은 즉각적인 거래가 가능하다는 오프체인의 장점을 활용한 실시간 비디오 스트리밍 시스템이다. 채널 상에서 실시간으로 1초당 이용 금액을 지불하고 1초의 비디오를 스트리밍

받는 것을 반복한다. 이러한 구조는 한번에 전체 서비스에 대한 비용을 지불하지 않기 때문에 서비스 도중 서비스가 중단 되는 것에 대한 대처가 유연하다. 전체 서비스에 대한 비용을 한번에 지불하게 되면 서비스 도중 서비스가 중단되었을 때 제공 받지 못한 서비스에 대해 서비스 제공자가 사용자에게 환불 금액을 송금해야 한다. 이 때 환불 과정에서 서비스 제공자가 책임을 회피할 수 있다. 또한 환불 금액을 측정하기 위해 서비스가 중단되기 전 서비스가 얼마나 이루어졌는지 파악하는 과정에서 분쟁이 발생할 수 있다. 오프체인을 활용한 실시간 비디오 스트리밍 시스템은 실시간으로 서비스 비용을 나누어 내며 이러한 단점을 극복할 수 있다. 서비스 도중 서비스가 중단되면 중단되기 전까지 이용한 서비스에 대한 금액만큼만 지불 했기 때문에 환불이 필요하지 않다.

오프체인 비디오 스트리밍 시스템은 예치금 입출금, 채널 오픈, 그리고 서비스 및 잔액 증명 세 단계로 이루어진다.

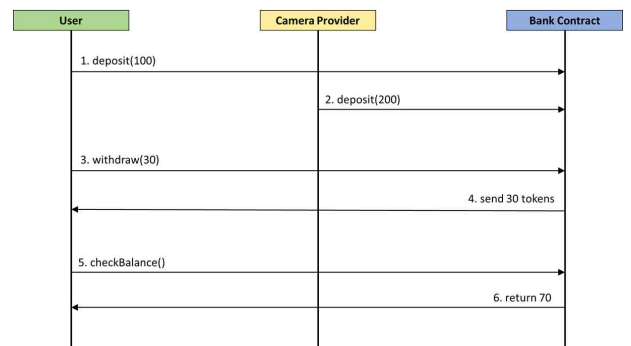


그림 1. 예치, 출금 및 잔액 확인 과정

그림 1은 오프체인 비디오 스트리밍 시스템에서 사용되는 예치금을

예치, 출금 및 잔액 확인을 하는 과정이다. 사용자와 서비스 제공자는 *deposit()* 함수를 통해 오프체인 거래 시 사용할 예치금을 은행 컨트랙트에 각각 100 토큰, 200 토큰씩 예치한다(그림 1.1, 그림 1.2). 사용자는 *withdraw()* 함수를 통해 예치했던 100 토큰 중 30 토큰을 출금 신청을 하고(그림 1.3), 은행 컨트랙트는 사용자에게 30 토큰을 전송한다(그림 1.4). 사용자는 잔액 확인을 위해 은행 컨트랙트에 *checkBalance()* 함수로 잔액 확인을 요청하고(그림 1.5), 은행 컨트랙트는 현재 사용자는 70 토큰을 보유하고 있다고 확인해준다(그림 1.6).

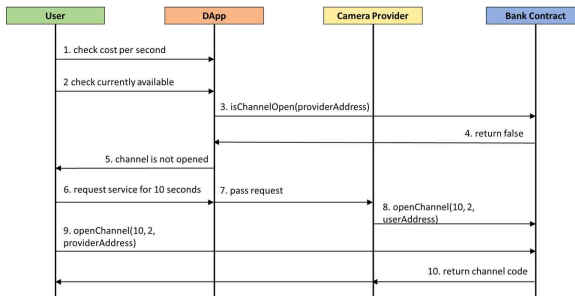


그림 2. 상태 채널을 여는 과정

그림 2는 사용자와 서비스 제공자가 오프체인 거래를 하기위한 충분한 예치금을 예치한 후 상태 채널을 여는 과정이다. 사용자는 서비스를 이용하기 위한 초당 금액을 Dapp을 통해 확인한다(그림 2.1). 서비스를 이용하기로 결정한 후 Dapp을 통해 현재 서비스가 이용 가능한지 확인한다(그림 2.2). Dapp은 은행 컨트랙트에 *isChannelOpen()* 함수를 통해 현재 서비스 제공자가 다른 채널을 통해 서비스를 제공 중인지 확인한다(그림 2.3). 현재 서비스 제공자는 다른 채널을 통해 서비스 중이지 않으므로 은행 컨트랙트는 Dapp에 채널이 열려있지 않다고 답한다(그림 2.4). 사용자는 서비스 제공자의 서비스가 현재 이용 가능하다는 것을 Dapp을 통해 확인하고(그림 2.5), 10초간 서비스를 이용하겠다는 요청을 Dapp에게 전달한다(그림 2.6). Dapp은 사용자로부터 받은 요청을 서비스 제공자에게 전달한다(그림 2.7). 사용자와 서비스 제공자는 서비스 시간, 초당 금액, 서로의 이더리움 계정 주소를 *openChannel()* 함수에 담아 은행 컨트랙트에 전달한다(그림 2.8, 그림 2.9). 은행 컨트랙트가 사용자와 서비스 제공자 모두에게 채널 오픈 요청을 받으면 사용자가 서비스를 이용하기에 충분한 예치금을 지니고 있는지 확인한 후 채널을 열고 사용자와 서비스 제공자만 입장 가능하도록 채널 코드를 반환한다(그림 2.10).

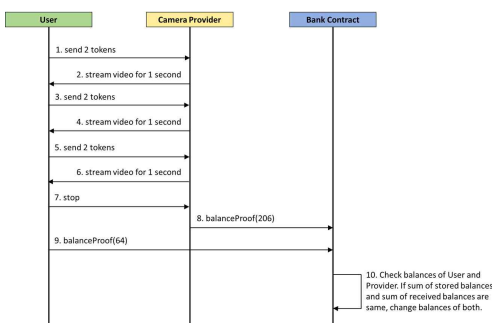


그림 3. 오프체인 채널 상 스트리밍 서비스 과정

그림 3은 채널을 오픈한 후 채널 상에서 비디오를 스트리밍하는 과정이다. 사용자는 70토큰, 서비스 제공자는 200토큰을 가지고 있다고 가정한다. 채널이 오픈되고 사용자가 1초당 금액을 보내면(그림 3.1) 1초간 비디오를 스트리밍 한다(그림 3.2). 사용자가 서비스 받기로 한 10초 동안 반복해서 1초당 금액을 보내고(그림 3.3, 그림 3.5) 서비스 제공자는 토큰을 받으면 1초간 비디오를 스트리밍 한다(그림 3.4, 그림 3.6). 서비스 도중 에러가 발생하거나 사용자가 서비스 중단을 원할 경우 서비스를 중단한다(그림 3.7). 서비스가 중단이 되면 사용자와 서비스 제공자는 *balanceProof()* 함수를 통해 각자의 잔액 증명을 요청한다(그림 3.8, 그림 3.9). 서비스 과정에서 사용자는 6 토큰을 사용해 잔액이 64 토큰이 되었고, 서비스 제공자는 사용자로부터 6 토큰을 받아 206 토큰이 되었다. 잔액 증명을 요청받은 은행 컨트랙트는 서비스 전의 사용자와 서비스 제공자의 잔액 합인 270(70+200) 토큰과 서비스 후 잔액 증명을 통해 전달 받은 잔액의 합인 270(64+206) 토큰이 일치함을 확인한 후 은행 컨트랙트 내의 사용자와 서비스 제공자의 잔액을 각각 64와 206로 수정한다.

3. 결론 및 향후 연구

오프체인 트랜잭션을 이용하여 블록체인의 한계를 극복한 오프체인 비디오 스트리밍 시스템을 제안했다. 실시간 거래가 가능한 오프체인 트랜잭션을 통해 기존 블록체인 거래의 단점을 극복하여 새로운 형태의 실시간 비디오 스트리밍 시스템을 설계하였다.

향후 설계된 시스템을 토대로 한 실제 구현이 필요하다. 또한 오프체인 채널과 블록체인 간 통신하는 과정에서 필요한 보안기술에 대한 추가적인 연구가 필요하다.

감사의 글

본 논문은 2020년 정부(과학기술정보통신부)의 재원으로 한국연구재단의 지원을 받아 수행된 연구임 (1711107567, 사용자 학습 유형을 고려한 360°VR 감각효과 휴먼팩터 연구)

참고문헌

[1] 정민혁, 김상균, “블록체인 기반 미디어사물인터넷 카메라 스트리밍 시스템.” 한국방송미디어공학회 학술발표대회 논문집, pp.292-294, 2019.
 [2] S.Dziembowski, S. Faust, and K. Hostáková, “General State Channel Networks,” CCS '18: Proceedings of the 2018 ACM SIGSAC Conference on Computer and Communications Security, pp.949-966, 2018.