

블록체인과 NFT 를 활용한 아이템 현금 거래 사기 방지 게임 개발

길선아¹, 이나운¹, 장윤주¹, 최은주¹, 김성욱²

¹서울여자대학교 정보보호학과 학부생

²서울여자대학교 정보보호학과 교수

{queenesun, wfg89, jjy784212, eun2001, kim.sungwook}@swu.ac.kr

Development of a Blockchain-based NFT Game to Prevent Cash Transaction Fraud

Sun-Ah Kil¹, Na-Yun Lee¹, Yoon-Ju Jang¹, Eun-Joo Choi¹, Sung-Wook Kim²

^{1,2} Dept. of Information Security, Seoul Women's University

요 약

기존 중앙 집중형 게임의 주요 문제로 아이템 현금거래 사기 범죄가 대두된다. 블록체인의 탈중앙화와 투명성, 불변성을 기반으로 게임이 운영된다면 문제를 해결할 수 있을 것이다. 본 논문에서는 블록체인 기술을 사용한 NFT(Non-Fungible Token) 게임을 제안한다. 인게임 재화는 모두 ERC-20 토큰으로, 아이템은 모두 ERC-721 토큰으로 생성하여 고유한 아이템을 이용자가 소유한다. 이러한 블록체인 기반 아이템 소유권은 안전한 아이템 거래 기능을 제공한다.

1. 서론

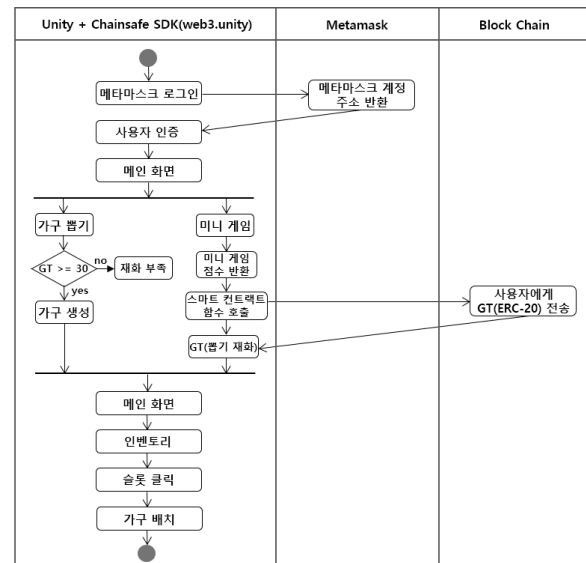
온라인 게임 관련 범죄 중 아이템 현금거래 시 발생하는 사기 범죄는 전체 사이버범죄의 약 46%에 해당한다. 이는 이용자가 특정 게임에서 보유한 아이템을 현금화할 목적으로 아이템 거래 중개 사이트를 통해 거래하는 과정에서 발생하며, 게임사들은 아이템의 소유권을 행사하며, 현금거래를 금지하고 있기에 이용자는 사기 피해 발생 시 구제받기 쉽지 않고 아이템에 대한 자유로운 권익 행사가 불가능하다. [1][2]

따라서 본 논문에서는 블록체인 기술을 활용한 Non-Fungible Token(이하 NFT) 게임 ‘D-ROOM’을 개발하였다. 게임 내 모든 아이템은 NFT로, 고유한 디자인의 복제 불가능한 아이템이 이용자의 소유가 되어 자유로운 권익 행사가 가능하다. 블록체인 기술은 분산 네트워크를 통해 거래에 대한 투명한 기록을 유지하고, 거래의 투명성과 가시성을 확보할 수 있으므로 거래 정보와 물품의 흐름을 실시간으로 추적할 수 있어 거래 참여자 간의 신뢰 문제를 개선하는 데 도움이 된다. 또한 블록체인 기반 스마트 계약을 통해 거래를 자동으로 실행시킴으로써 계약불이행에 따른 분쟁을 방지할 수 있다. 이를 게임에 적용하는 경우 기존 게임 시스템에서 발생하는 아이템 현금 거래 사기 피해를 방지할 수 있다. [3]

2. 설계 및 구현

2.1. 시스템 구성도

본 논문에서 제안하는 NFT 게임은 게임 이용자와 Unity, Chainsafe SDK, Metamask, Ethereum 블록체인 네트워크의 상호작용을 통해 작동한다. Smart Contract는 Remix Ethereum IDE에서 동작하며, Chainsafe web3.unity SDK 오픈소스를 활용해 Unity와 연동하였다. Web 3.0 환경 구축을 위해 Chainstack을 사용하였다. 개발 언어는 C#과 Solidity를 사용하였다.



(그림 1) 시퀀스 다이어그램.

그림 1 은 본 게임의 전체 실행 순서도를 보여준다. 구체적으로, 게임을 실행하면 이용자로 하여금 Metamask 지갑을 통해 로그인하도록 한다. 로그인 시 불러온 Ethereum 계정 주소로 블록체인 네트워크에서 사용자를 인증하며, 게임 내에서 거래 등의 행위를 하게 되면 트랜잭션 데이터가 생성되어 블록체인에 전송된다. 블록체인 네트워크에서는 해당 트랜잭션을 검증하고 Smart Contract 를 실행해 그 결과를 기록한다. 이후 Unity 게임 클라이언트가 갱신되어 실시간으로 게임 상태를 반영한다.

2.2 게임 화면 구성

게임 화면 구성은 그림 2 와 같다. 게임 실행 후 로그인을 진행하면 메인 화면으로 이동한다. 메인 화면에서는 소유하고 있는 가구 아이템을 방에 배치할 수 있으며, 우측 하단의 버튼을 통해 미니게임, 거래소, 인벤토리, 가구 뽑기 화면으로 이동할 수 있다.



(그림 2) 메인 화면 구성

미니게임은 인게임 재화 공급을 위해 존재한다. 가구 뽑기는 재화를 소비하여 가구 NFT 를 획득할 수 있다. 중복되지 않는 조합의 가구 생성을 위해 Unity 상에서 마스킹 처리 기법을 사용하였다.

2.3. Smart Contract

Smart Contract 는 크게 ERC-20 토큰 발행, ERC-721 토큰 발행, 게임 내 기능 구현 Contract 로 구분된다.

(1) GameToken Contract (ERC-20 토큰 발행과 지급)

인게임 재화인 ERC-20 토큰(이하 GT)은 GameToken Contract 를 Remix 에서 배포하는 순간 코드상에서 명시된 만큼의 GT 가 개발자의 메타마스크 계정으로 지급된다. 이후 개발자 계정에서 Game Contract 로 GT 를 전송하여 이용자가 미니 게임 보상을 획득할 때마다 Game Contract 로부터 GT 를 전달받을 수 있도록 한다.

(2) Furniture Contract(IPFS 통한 ERC-721 토큰 발행) 블록체인 구조상 대량의 데이터를 저장하는 데 적합하지 않다. 대량의 데이터를 모든 노드가 저장하고 유지해야 하는데 모든 노드가 동일한 데이터를 보유하는 것은 네트워크 대역폭 및 저장 공간을 비효율적으로 만든다. 따라서 본 논문에선 IPFS 기술

을 사용하였다. IPFS 는 P2P 방식으로 분산 파일 시스템에 데이터를 저장하고 Web 상에 공유하기 위한 프로토콜 네트워크이다.[4]

게임 아이템 이미지를 NFT Storage 에 Metadata 형태로 업로드하여 API key 값을 얻는다. 이를 NFT Storage 에 안내된 코드에 넣어 JSON 형식의 파일을 포함한 IPFS hash link 를 얻는다. 해당 hash link 를 Smart Contract 상에서 가져와 민팅을 진행하여 ERC-721 토큰 형태의 아이템을 생성하게 된다.[5]

(3) Game Contract (게임 내 기능 구현)

미니게임이 끝나면 playMiniGame 함수를 호출하여 획득한 점수를 함수 인자로 넘긴다. 점수 1 점당 GT 1 개로 환산되어 이용자의 계정 주소로 GT 가 지급된다. 이용자 계정으로 미니 게임을 진행한 후 GameToken Contract 의 balanceOf 함수를 통해 잔액을 확인하면 그림 2 와 같이 점수만큼 환산된 29GT 가 성공적으로 지급된 것이 확인된다.

이용자는 GT 를 사용하여 가구를 뽑을 수 있다. 인게임 가구 뽑기 버튼을 누르면 buyFurniture 함수가 실행되며, 해당 함수 내에서 Furniture Contract 를 호출하여 새로운 ERC-721 토큰을 발행해 이용자의 인벤토리로 지급한다.

3. 결론 및 향후 과제

본 논문은 블록체인 기술을 기반으로 한 NFT 게임 서비스 개발에 대해 다루었다. 게임 아이템 소유권의 문제와 그에 따른 사기 피해를 줄이고자 게임 이용자가 중심이 되는 게임 서비스를 구축하고자 하였다. 향후 Unity 마스킹 기법을 통해 생성되는 모든 아이템을 순차적으로 토큰화하는 작업과 더불어 이용자 간 자유로운 거래를 위한 인게임 거래소 구현 작업을 통해 더욱 자율적인 게임 경제 시스템을 구축할 수 있을 것으로 기대한다.

※ 본 연구는 교육부 및 한국연구재단 대학혁신지원 사업으로부터 지원받은 연구임(2024)

참고문헌

- [1] 유용봉, 온라인 게임범죄의 사례분석과 대응방안, 한국콘텐츠학회논문지, 제 6 권, 제 9 호, 87, 2006.
- [2] 신영수, 온라인게임 이용자보호와 약관규제, IT 와 법연구, 4, 221-250, 2010.
- [3] 최철호 외, 신용장거래 사기방지를 위한 블록체인 기술의 적용, 국제상학, 3-21, 2020
- [4] 강성준 외, IPFS 기반의 블록체인 스토리지 방법, Proceedings of KIIT Conference, 454-458, 2023.
- [5] <https://nft.storage/>