분산화와 투명성 확보를 위한 블록체인 기반 모바일 오더 시스템 설계

이민규[1] 박정진[O2] 박기석[1]

[1]인천대학교 컴퓨터공학부

[2]인천대학교 물리학과

{mingyu[1], rednoy03[O2], gspark[1]}@inu.ac.kr

Design and Implementation of a Blockchain-Based Mobile Order System for Decentralization and Transparency

Mingyu Lee[1] Jeongjin Park[O2] Giseok Park[1]

[1]Department of Computer Science and Engineering, Incheon National University

[2]Department of Physics, Incheon National University

{mingyu[1], rednoy03[O2], gspark[1]}@inu.ac.kr

요 약

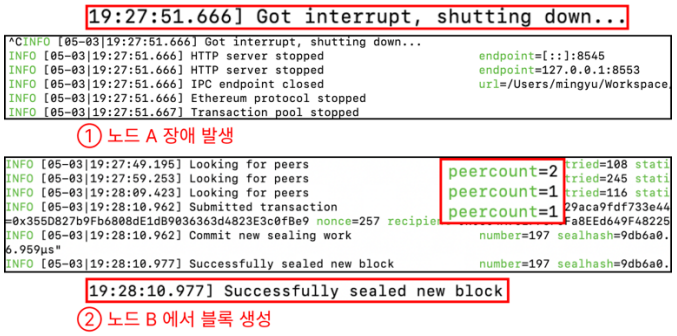
본 논문에서는 시스템 다운타임, 데이터의 불투명성, 데이터 조작에 대한 민감성 등 기존 중앙집중식 서버 시스템의 한계를 해결하기 위해 블록체인 기반 모바일 오더 시스템을 제안한다. 제안된 시스템은 블록체인의 탈중앙화 구조를 통한 투명성을 강화함으로써 시스템 가용성을 향상시키고 데이터 무결성을 보장한다. 권한 증명 합의 알고리즘에 속하는 Clique 방식을 통해 확장성을 높여 트랜잭션 처리의 이점을 얻고, NFT 발급을 활용하여 조직 내 신원 확인 기능을 제공한다. 추가적으로, 스마트 컨트랙트를 통해 안전하고 투명한 거래를 제공한다.

1. 서 론

현재 대부분의 서비스는 중앙집중식 시스템으로 하나의 서버에서 사용자의 요청을 처리한다. 이를 통해, 빠른 처리가 가능하지만, 중앙 서버의 과부하나 장애로 인해 전체 서비스가 중단될 위험이 높다. 또한, 외부의 악의적인 개입이나 내부의 오류에 의한 데이터 위조 및 변조는 서비스 신뢰성을 감소시킬 수 있다.

블록체인은 P2P(Peer-to-Peer) 네트워크에서 관리되는 자산의 디지털 원장 기술이다[1]. 데이터의 분산 저장, 불변성, 투명성 등의 장점으로 인해 다양한 산업 분야에서 블록체인 기술이 채택되고 있다[2]. 투명성과 무결성을 확보한 결제 시스템은 고객의 신뢰를 얻을 수 있다.

본 논문에서는 기존의 중앙집중식 서버 시스템 기반의 모바일 오더 앱이 갖는 시스템 다운타임, 데이터 불투명성 및 변조 가능성의 문제점을 개선하기 위해 블록체인 기반 모바일 오더 시스템을 제안한다.



[그림 1] 블록체인 동작 화면

본 논문의 구성은 다음과 같다. 2장에서는 블록체인 기술의 주요 특징에 대해 소개하고, 3장에서는 모바일 오더 앱에 블록체인 기술이 적용되는 구체적인 방안을 제시한다. 4장에서는 블록체인 기술이 적용된 모바일 오더 앱의 설계 과정을 제시하고, 5장에서는 결론을 맺고 향후 연구 방향을 제시한다.

2. 블록체인 기술의 특징

제안하는 시스템을 기술적으로 구현하기 위해 블록체인 기술을 적용하였다. 블록체인은 다음과 같은 특징을 갖는다.

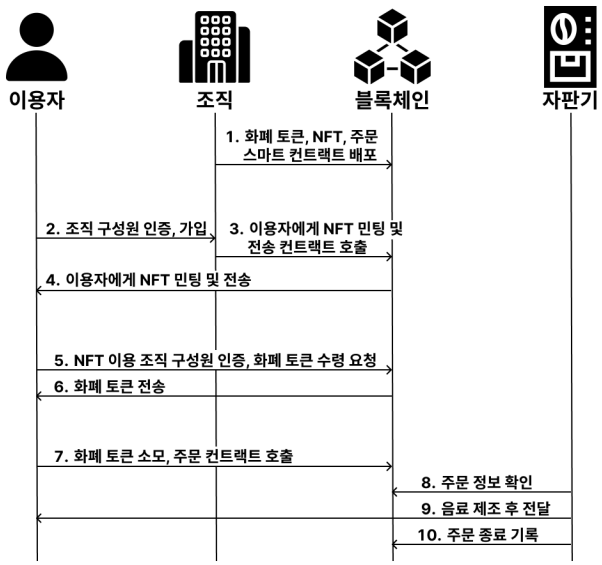
- 분산성(Distribution): 블록체인은 분산 시스템으로 노드 간 연결을 통해 네트워크를 구성하여 단일 장애 지점(single point of failure) 문제를 해결할 수 있다.
- 무결성(Integrity): 발생한 거래 정보는 각 노드의 분산 장부에 기록되어 데이터 위변조가 불가능하다.
- 투명성(Transparency): 블록체인에 기록된 데이터는 누구나 확인 가능하고, 데이터의 실시간 검증이 가능하여 데이터의 신뢰성을 향상시킨다.

블록체인은 중앙집중화 시스템과 달리, 네트워크 참여 노드들 간 연결을 통해 네트워크를 구성한다. 또한, 블록체인에 기록된 데이터는 변경이 불가능하여 데이터 신뢰성을 보장한다. 스마트 컨트랙트(smart contract)는 블록체인 내에 배포되어 실행되는 자동화된 계약이다. 이를 통해 중간자 없이 사용자 간 거래가 가능하고, 오류 발생률을 감소시킨다.

3. 블록체인 기술 적용 방안

이 연구에서는 다음의 상황을 가정한다.

1. 조직 구성원이 화폐로 이용될 토큰을 수령하길 요청하면 토큰을 지급한다.



[그림 2] 블록체인을 활용한 모바일 오더 시스템 아키텍처

2. 구성원은 해당 토큰을 이용하여 주문을 실시한다.
3. 자판기에서 음료를 제공한다.

제안하는 시스템은 권한 증명(Proof-of-Authority, PoA)에 속하는 Clique 방식 기반의 합의 알고리즘이 비공개형 네트워크에 적용되었다. Clique는 미리 선정된 다수의 노드들이 순차적으로 블록을 생성하고 검증하는 역할을 함으로써 신속한 트랜잭션 처리가 가능하다. 또한, 일부 노드에 문제가 발생해 역할을 수행할 수 없게 되어도, 나머지 노드들이 정상적인 네트워크 운용을 가능하게 한다. 이에 대한 동작 화면을 [그림 1]에 나타냈다. 추가적으로, 블록 제안자가 되기 위해 복잡한 수학적 문제를 풀어야 하는 작업 증명(Proof-of-Work, PoW) 합의 메커니즘에 비해 에너지 효율이 매우 높아, 노드 운영에 사용되는 비용을 감소시킬 수 있다.

조직 구성원의 소속 인증은 NFT(Non-Fungible Token) 기술을 통해 해결하였다. NFT는 대체 불가능한 속성을 갖고 있으며, NFT의 소유권은 공개적으로 확인할 수 있도록 블록체인에 저장된다. 조직의 관리자는 각 구성원에게 고유한 NFT를 발급할 수 있고, 구성원은 NFT의 소유권을 증명함으로써 소속을 인증한다. 따라서, 구성원은 모바일 오더에 필요한 화폐의 역할을 하는 토큰을 발급받을 수 있다. 블록체인 네트워크에서 발급된 NFT는 변조가 불가능하기 때문에, 제3자가 거짓으로 신원 인증하는 것을 방지할 수 있다.

모든 계정의 토큰 보유 정보와 거래 내역은 장부에 저장되고 투명하게 공개되어 누구나 확인 가능하다.

결과적으로, 데이터 제공자를 신뢰하지 않고 검증하는 무신뢰(trustless) 시스템을 달성할 수 있다.

토큰 수령과 주문 기능은 네트워크에 배포된 스마트 컨트랙트에 의해 실행되므로, 실행 결과는 예상이 가능하며 오류 발생 가능성이 적다.

4. 시스템 설계

제안하는 시스템을 기술적으로 구현하기 위해 세 종류의 스마트 컨트랙트를 배포하였다.

첫 번째로, 이용자 인증을 위한 NFT 스마트 컨트랙트를 배포했다. 해당 스마트 컨트랙트는 배포한 주체인 조직만이 발행 및 전송 컨트랙트를 호출할 권한을 갖고, 이 NFT를 소유한 이용자는 조직 구성원임을 인증할 수 있다.

두 번째로, 주문을 위한 가상 화폐 토큰 스마트 컨트랙트를 배포했다. 주문에 사용되는 가상 화폐는 구성원만 수령 요청을 할 수 있어, 조직 구성원 이외의 이용자가 수령 요청하는 것을 방지할 수 있다. 토큰 수령 요청 컨트랙트에 시간당 요청 횟수 제한 등 조건을 설정할 수 있어, 무분별한 수령 요청 호출을 막을 수 있다.

세 번째로, 자판기에 주문을 입력하기 위한 주문 스마트 컨트랙트를 배포했다. 주문 컨트랙트에는 저장소에 주문할 수 있는 음료의 종류와 가격을 설정하여, 정상적인 음료 메뉴인지 유효성 검사가 가능하다. 따라서, 화폐 토큰을 소모하도록 만들 수 있다. 자판기에서는 주문 정보를 확인하고 음료를 전달한 이후에 주문 종료를 기록한다.

[그림 2]는 제안하는 시스템의 동작 순서를 나타낸다. 이에 대한 자세한 설명은 다음과 같다. 1) 조직은 각 스마트 컨트랙트를 블록체인에 배포한다. 2) 조직의 이용자는 서비스를 사용하기 위해 자신의 정보를 조직에 전달한다. 3) 조직은 이용자가 조직 구성원임을 확인하고, 이용자를 위한 NFT를 발행한다. 4) 발행된 NFT는 이용자에게 전달된다. 5) 이후, 이용자는 주문을 위한 가상 화폐 토큰을 요청한다. 6) 가상 화폐 스마트 컨트랙트는 이용자 NFT 인증 후, 가상 화폐를 발급한다. 7) 이용자는 발급받은 가상 화폐를 지불하여 음료를 주문한다. 8) 자판기는 주문 정보를 확인한다. 9) 확인된 주문 정보를 바탕으로 음료를 제조하여 전달한다. 10) 이후 자판기는 주문 종료 트랜잭션을 실행한다.

이용자는 블록체인 네트워크에 노드로 참여해 동기화하거나 블록 탐색기를 이용함으로 블록체인에 기록된 정보를 자유롭게 조회할 수 있다.

5. 결론

본 논문은 블록체인 기반의 모바일 오더 시스템을 제안한다. 제안하는 시스템은 PoA 기반의 블록체인을 활용하여 탈중앙화 구조와 투명성을 확보해 시스템 가용성과 데이터 신뢰성을 보장한다.

누구든지 노드를 직접 운용하면 데이터를 검증하는 것이 가능하지만, 노드 운용에는 상당한 하드웨어 비용과 유지 보수에 노력이 필요하다. 따라서 많은 이용자가 매우 적은 비용으로 직접 데이터를 검증할 수 있도록 하는 라이트 클라이언트를 적용하는 것이 향후 연구 과제이다[3].

또한, 데이터가 투명하게 공개되는 것은 데이터 위변조 방지와 증명의 이점을 얻을 수 있지만, 익명성이 보장되지 않는다는 위협이 존재한다. 따라서 정보 자체는 공개하지 않고 정보를 증명할 수 있도록 하는 영지식 증명(Zero-Knowledge Proof)의 활용은 익명성을 확보한다[4]. 이를 통해 블록체인 기반의 보안성이 높은 멤버쉽 결제 시스템 상용화에 기여하고자 한다.

참고문헌

[1] S. Nakamoto, "Bitcoin: A Peer-to-Peer Electronic Cash System", https://bitcoin.org/bitcoin.pdf, 2008.

[2] S. Markus and P. Buijs, "Beyond the hype: how blockchain affects supply chain performance.", Supply Chain Management: An International Journal 27.7, 2022.

[3] V. Buterin, "Light Cleints and Proof of Stake", https://blog.ethereum.org/2015/01/10/light-clients-proof-stake, 2015.

[4] Goldwasser, Shafi, Silvio Micali and Chales Rackoff, "The knowledge complexity of interactive proof-systems.", Providing sound foundations for cryptography: On the work of shafi goldwasser and silvio micali, 1989.