2024년 전기 졸업과제

스마트 컨트랙트 및 프라이빗 블록체인을 활용한 커피 물류 관리 시스템 구현

개요

커피는 더 이상 단순한 기호 식품이 아니라 일상의 필수적인 부분이 되어 우리 문화에 깊게 자리 잡고 있다. 현대인들에게는 커피를 마시는 것은 하루를 시작하는 일상이 되었으며, 식사 후에 졸음을 이기고 두뇌를 깨우는 데 필요한 것으로 인식되어 있다. 또한 커피를 마시면서 업무 혹은 학업을 하고, 사람들 간에 대화하는 등 습관처럼 일상에서 소비되고 있다.

이처럼, 커피는 한국뿐만 아니라 전 세계에서 상당히 큰 비중을 차지하고 있는 산업이다. 그러나 현재 커피 물류 시스템에서는 장시간 노동에 대한 적절한 임금을 받지 못하는 농부가 존재하며, 선호하는 원두를 소비하지 못하고 낮은 품질의 원두를 소비하는 소비자가 종종 존재한다. 이에 스마트 컨트렉트와 프라이빗 블록체인을 활용하여, 보안과 신뢰성, 투명성 그리고 효율성까지 확보하고자 한다. 또한 현재 택배 및 배송 업체들이 겪고 있는 원산지 확인, 물류 추적 등과 같은 문제를 해결하는 시스템을 구현하고자 한다.

목차

1. 연구 배경

a) 배경

한국에서 커피 소비는 최근 몇 년 동안 상당한 증가세를 보이는 중이다. 유로모터스에 따르면 2023년 국내 1인당 연간 커피 소비량은 405잔으로 전 세계 1인당 연간 커피 소비량 152잔 대비 두 배 이상 높았다. 식품의약품안전처에 따르면, 2022년 음료류 품목별 국내 판매액 중 전체 음료 시장에서 커피류가 차지하는 비중도 30.8%로 탄산음료 25.5%보다 높다. 2023년 전 세계 커피 시장 규모는 1,131억 5,260만 달러로 전년 대비 9.0% 증가했고, 2027년까지 연평균 4.3% 성장해 1,331억 5,750만 달러로 확대될 전망이다. 이처럼 전 세계적 커피 시장의 흐름은 확대될 것으로 예측된다.

커피 원두는 일반적으로 원산지를 기반으로 마케팅되며, 각 지역은 고유한 맛과 특성을 가진 커피를 생산하는 것으로 알려져 있다. 그러나 현재까지는 수작업을 통하여 원산지를 추적했기 때문에, 품질이 낮은 지역의 원두를 유명한 커피 재배 지역의 프리미엄 원두로 라벨링 되어 높은 가격을 책정하는 등 신뢰성이 부족하였다.

또한 농부에서부터 수출입업자, 도소매 업체 등 다분화된 공급망은 신뢰성 있는 원산지와 품질을 검증하는 것이 어려워지는 것에 동조한다. 그리고 커피의 최종 소비자뿐만 아니라 농부들 역시 투명성 및 시장 정보 부족으로 공정한 가격을 받지 못하여, 커피 농부들의 생계뿐만 아니라 커피 공급망의 전반에 품질과 지속 가능성에도 영향을 미친다.

b) 목표

이에 금융권에서 주로 사용하던 블록체인 기술을 커피 산업에서 활용하는 것은 커피 산업에 많은 이점을 줄 수 있다.
커피 공급망의 투명성과 추적 가능성을 개선하여 농부로부터 소매업체에 이르는 각 단계의 이해관계자가 커피 원두의 물류 과정을 정확히 파악함으로써, 도소매 업체가 원두의 품질에 맞는 합리적인 가격에 유통하도록

유도할 수 있다. 또한 최종 커피 소비자는 본인이 선호하는 원산지의 원두를 소비할 수 있으며, 가격에 상응하는 품질의 커피를 소비할 수 있게 유도할 수 있다.
본 연구는 스마트 컨트랙트 및 프라이빗 블록체인을 활용하여 복잡하고 불투명한 현재 물류 과정을 획일화하여, 투명성과 신뢰성을 부여하고자 한다. 추가로, 이 시스템을 통해, 실시간 물류 추적 및 오배송의 최소화를 목표로 한다.

2. 문제상황

a) 중앙화 문제

프라이빗 블록체인에서 중앙화의 문제는 권력이 중앙 기관이나 블록체인 소유자가 선택한 소규모 검증인 그룹에 의해 통제되는 경향이 있다. 이 구조는 네트워크의 결정 과정에서 모든 이해관계자의 참여를 보장하지 못하며, 특정한 그룹이 권력을 독점할 가능성이 높아진다. 이로 인해 네트워크의 운영과 정책 결정이 불투명해지고 비효율적일 수 있다.

b) 공격에 대한 취약성

프라이빗 블록체인의 검증인 수가 적은 것은 네트워크의 보안을 위협하는 요소다. 노드의 수가 제한적이기 때문에, 소수의 노드만이 합의 과정에 참여한다. 이는 네트워크가 외부 공격 또는 내부의 악의적인 행위에 대한 저항력이 약하다는 것을 의미하며, 특정 공격 유형에 특히 취약할 수 있다.

c) 검열 위험

프라이빗 블록체인은 중앙화된 통제하에 있기 때문에, 네트워크 운영자가 새로운 규칙이나 업데이트를 도입할 때 검열의 위험이 있다. 네트워크 운영자가 중앙 권한이 특정 트랜잭션을 차단하거나 불리한 정보를 제외할 수 있다. 충분한 수의 검증인이 이에 동의하면, 블록체인에 기록된 정보를 변경하거나 특정 정보의 기록을 막을 수 있으므로, 사용자의 신뢰성과 투명성이 저하될 수 있다.

3. 문제 상황 별 대응책

a) 분산된 권한 구조 도입

프라이빗 블록체인의 구조를 변경하여, 더 많은 참여자가 검증 과정과 결정권에 참여할 수 있도록 한다. 해당 네트워크에 대한 검증인의 수를 늘리고 다양한 이해관계자 그룹을 포함되게 함으로써 권력 집중을 방지하고자 한다.

b) 다중 인증 및 다층화된 보안 레이어 형성

네트워크에 접근할 수 있는 사용자를 엄격히 제한하고, 중요 작업에는 다중 인증을 요구함으로써 내부 공격에 대한 방어력을 높인다. 네트워크의 현재 상태를 주기적으로 확인하고, 예외적 움직임이 감지되면 곧바로 탐지하고 대응할 수 있게 한다.

또한 추가적인 보안 레이어를 구성하여 중요 정보를 별도의 보안이 강화된 네트워크 구간에 저장하는 다중 보안 레이어 프로토콜을 형성할 계획이다. 이와 같은 해결 방법들을 적용함으로써 프라이빗 블록체인의 네트워크 보안 문제를 최소화한다.

c) 다수결 기반의 통일된 합의 메커니즘 설정

특정 소수 참여자들의 개별적인 합의를 방지하기 위해 다수의 참여를 기반으로 한 통일된 합의 메커니즘을 형성한다. 거래 블록의 변경 및 추가 과정에서 다수의 참여자의 동의를 필요로 하는 규칙을 설정한다. 이는 모든 거래 업데이트에 대해 투명하고 획일화된 검토 방식을 제공할 수 있다.

4. 개발 환경 및 사용기술

a) 개발 환경

1. 개발 언어
- JavaScript (웹)
- Solidity (스마트 컨트랙트)
- Go (이더리움 네트워크 및 노드)

2. 개발 도구
- React (웹 개발)
- Web3.js (이더리움 노드와 상호작용)
- Remix IDE (스마트 컨트랙트 구현)
- Geth (이더리움 네트워크 구축 및 노드 생성)

3. 실행환경
- Node.js (개발 및 빌드)
- 웹 브라우저 (사용자 인터페이스 실행)
- EVM (스마트 컨트랙트 작성 및 테스트)
- Ethereum network (Geth로 설계)

b) 사용 기술

1. 스마트 컨트랙트

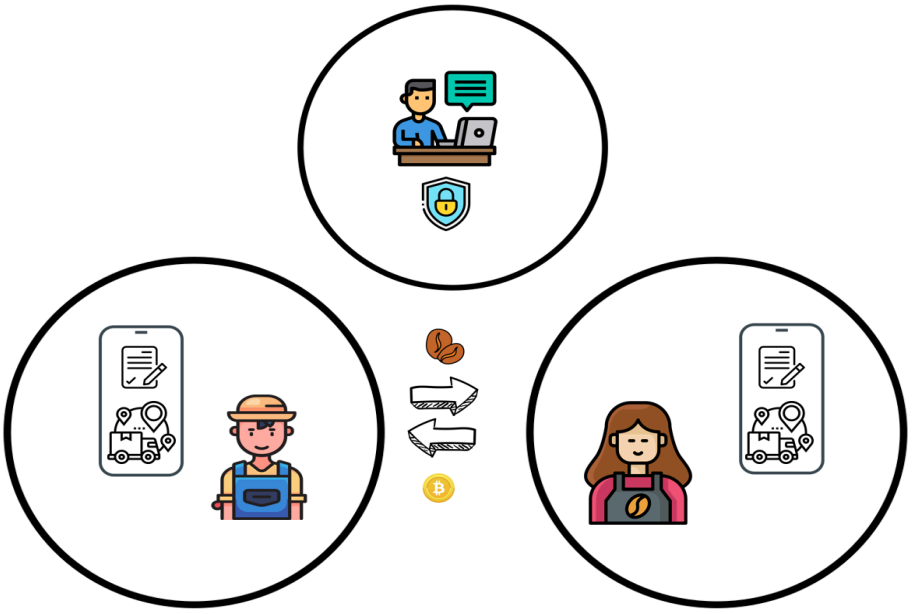
스마트 컨트랙트란 블록체인 기술을 활용해 제삼자 인증기관 없이 개인 간에 계약을 자동으로 체결하고 실행할 수 있도록 하는 기술이다.

기본적으로 이더리움 스마트 컨트랙트는 계약 코드와 두 개의 공개 키로 구성된다. 첫 번째 공개 키는 계약 작성자의 키이며, 두 번째 공개 키는 계약 자체를 나타내는 고유한 디지털 식별자이다.

스마트 컨트랙트 설계 시
1) 관측 가능성 (observability): 서로의 계약 이행 가능성을 관찰하거나 성과를 입증할 수 있어야 한다.
2) 검증 가능성 (Verifiability): 계약을 충족시키거나 위반하는 경우, 계약 당사자들이 이를 명확히 알 수 있어야 한다.

3) 개인정보 보호(Privity): 계약 내용은 계약 당사자들만 확인할 수 있도록 보호돼야 한다.
4) 강제 가능성(Enforceability): 계약이 의무적으로 이루어질 수 있게 구속력을 가진다.

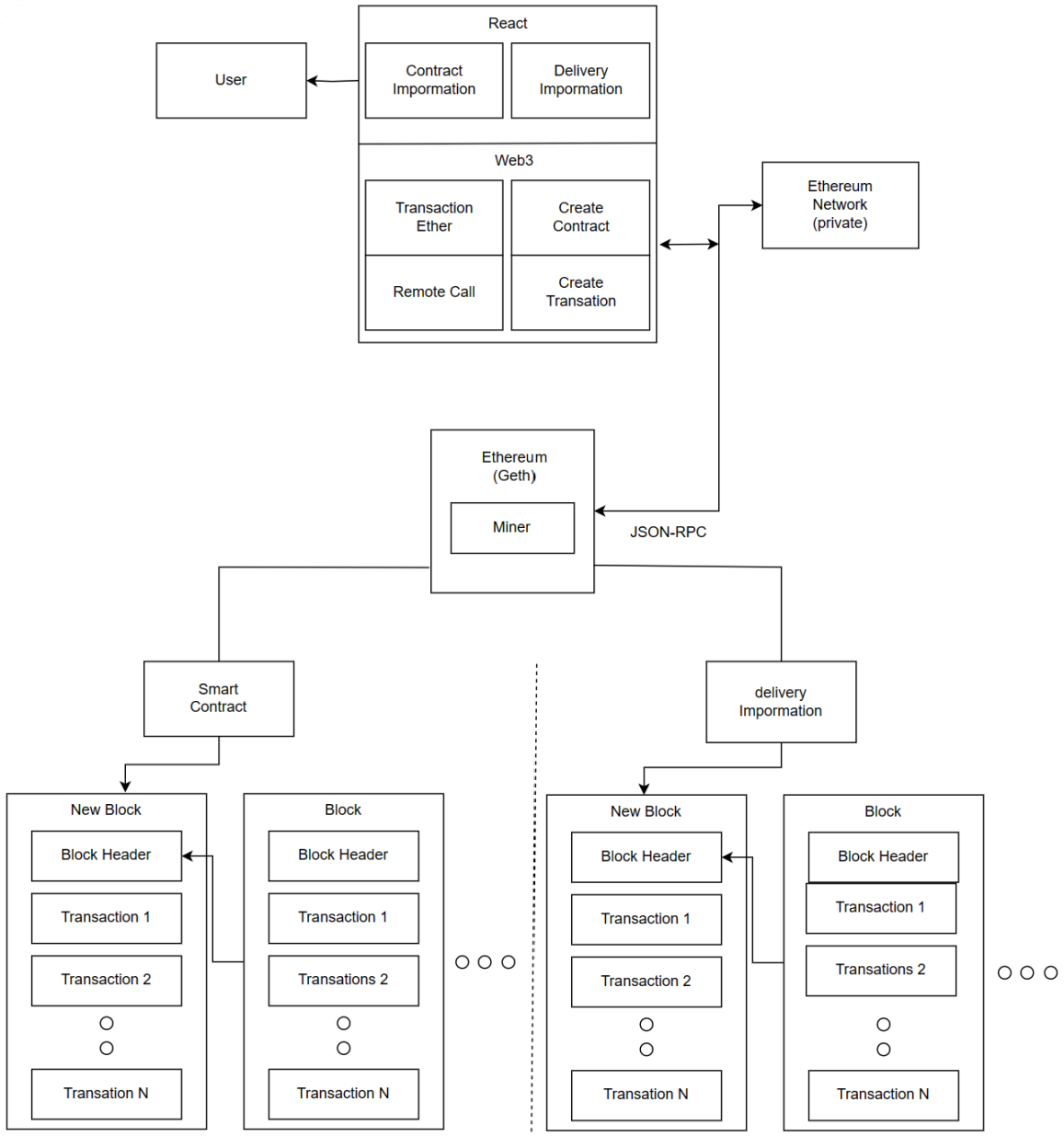
위의 네 가지 특징들을 모두 충족시키는지를 확인해야 한다.



2. 프라이빗 블록체인

프라이빗 블록체인(private blockchain)이란 미리 정해진 조직이나 개인들만 참여할 수 있는 폐쇄형 블록체인 네트워크를 말한다. 하나의 그룹에서 독자적으로 이용할 수 있으며 참여자가 제한된 특성을 가져 기관 간 거래 시스템을 형성하는 데 적합하다. 참여자가 적어 퍼블릭 방식보다 더 빠른 거래 속도를 제공하며 예기치 못한 금융 사고가 발생했을 시 책임 주체가 명확해짐으로써 금융 거래에 대한 신뢰성을 보장 받을 수 있다.

c) 시스템 구조



1. 데이터 입력

- 유저는 리액트로 구현된 웹사이트에서 계약 정보 또는 배송 정보를 입력한다.
- 입력된 정보는 백엔드 서버로 전송된다.
- 백엔드 서버는 Web3 라이브러리를 사용하여 스마트 컨트랙트를 호출하고, 입력된 정보를 포함하는 트랜잭션을 생성한다.
- 생성된 트랜잭션은 서명되어 프라이빗 이더리움 네트워크로 전송된다.

- 이더리움 네트워크의 노드는 트랜잭션을 검증하고 새로운 블록을 생성하여 블록체인에 추가한다.

2. 데이터 조회

- 유저는 React 웹사이트를 통해 저장된 계약 정보 또는 배송 정보를 조회한다.
- React 웹사이트는 백엔드 서버에 요청을 보내고, 백엔드 서버는 Web3 라이브러리를 사용하여 블록체인에서 데이터를 조회한다.

5. 일정 및 역할분담

a) 개발 일정

개발 구분	5					6				7				8					9			
	1	2	3	4	5	1	2	3	4	1	2	3	4	1	2	3	4	5	1	2	3	4
사전 자료 조사																						
블록체인 스터디																						
개발 프레임워크 스터디																						
블록체인 네트워크 구축																						
체인코드 개발																						
웹 **UI** 및 개발																						
테스트 및 수정																						
최종 점검 및 발표 준비																						

b) 역할 분담

학번	이름	구성원별 역할
201924586	조주영	이더리움 네트워크 구축 UI 디자인 / 설계 및 플랫폼 개발 백엔드 서버 개발
201924436	김영목	이더리움 가상환경 구축 이더리움 네트워크 구축 체인코드 및 서버 개발
201941171	장영철	이더리움 네트워크 구축 체인코드 및 서버 개발 블록체인 관리
공통		사전 자료조사 관련 논문 분석

6. 참고문헌

- [초점] '대한커피민국' 1인당 연간 405잔 마신다...세계 평균 2.5배 http://www.newsian.co.kr/news/articleView.html?idxno=66185
- GOPAX ACADEMY. "퍼블릭 블록체인과 프라이빗 블록체인이 무엇인가요?"
- BTCC. "스마트 컨트랙트란 무엇입니까?"
- 해시넷. "프라이빗 블록체인"
- 이은주,and 김진욱. "이더리움 기반 공공정보 소프트웨어 사업산출물관리 시스템 설계 및 구현." 정보처리학회논문지. 컴퓨터 및 통신시스템 11.6 (2022): 177.