**서론**

**1.1 연구 배경 및 필요성**

현대 사회에서 디지털 금융 서비스는 급속히 발전하고 있으며, 이에 따라 개인 간(Peer-to-Peer, 이하 P2P) 자금 이동에 대한 수요 또한 증가하고 있다. 특히, 중앙 기관에 대한 의존 없이 개인 간 직접적인 송금이 가능한 시스템에 대한 요구가 높아지고 있다. 기존 금융 시스템은 신뢰성 있는 중개 기관을 필요로 하나, 이는 추가적인 비용과 시간 소요를 유발하며, 중앙 시스템의 장애나 보안 위협에 노출될 수 있는 단점을 지닌다. 이러한 한계를 극복하기 위한 대안으로, 블록체인 기반의 P2P 송금 시스템이 주목받고 있다.

블록체인은 탈중앙화, 불변성, 투명성 등의 특성을 통해 제3자의 개입 없이도 안전하고 신뢰할 수 있는 거래를 가능하게 한다. 이에 따라 본 논문에서는 블록체인 기술을 활용하여 사용자 간 직접 송금을 지원하는 시스템을 설계하고, 그 구현 결과를 검증하고자 한다.

**1.2 블록체인 기반 결제 시스템의 장점과 한계**

블록체인 기반 결제 시스템은 거래 기록이 모든 참여자에게 공유되며, 변경이 불가능한 형태로 저장되기 때문에 데이터의 무결성과 투명성을 보장할 수 있다. 또한, 중앙 기관이 존재하지 않기 때문에 시스템 장애 가능성이 줄어들고, 거래 수수료를 절감할 수 있다는 장점이 있다.

그러나 블록체인 기반 시스템은 트랜잭션 처리 속도, 확장성 문제, 스마트컨트랙트 취약점 등 여러 한계점을 내포하고 있다. 특히 스마트컨트랙트 상의 보안 취약성은 금전적 손실로 이어질 수 있어, 설계 및 개발 단계에서 충분한 검토와 방어 기법 적용이 필요하다.

**1.3 연구 목표 및 논문의 구성**

본 연구의 목표는 블록체인 기술을 기반으로 하는 P2P 송금 시스템을 설계하고 구현함으로써, 사용자 간 직접적인 송금을 안전하게 지원하는 스마트컨트랙트를 개발하는 것이다. 특히, 이중 지불 방지 및 재진입 공격 방지 등 보안 요소를 고려한 설계를 통해, 실질적인 시스템의 신뢰성과 안전성을 검증하는 데 중점을 둔다.

논문의 구성은 다음과 같다.  
2장에서는 블록체인과 스마트컨트랙트에 대한 이론적 배경을 서술하며, 기존 P2P 결제 시스템과의 차이점을 분석한다. 3장에서는 본 연구에서 설계한 P2P 송금 시스템의 아키텍처와 스마트컨트랙트 구조를 설명한다. 4장에서는 구현 및 실험 과정을 기술하고, 개발된 시스템의 기능적 검증 결과를 제시한다. 5장에서는 시스템의 보안성 및 성능 분석을 통해 연구 결과를 종합적으로 평가한다. 마지막으로 6장에서는 본 연구의 한계점을 논의하고 향후 연구 방향을 제시한다.

**2. 이론적 배경**

**2.1 블록체인의 기본 개념**

블록체인은 분산 원장 기술(Distributed Ledger Technology, DLT)의 일종으로, 거래 기록을 다수의 참여자가 공유하는 형태로 저장하는 시스템이다. 블록체인에서는 새로운 거래 데이터가 일정 시간마다 블록 단위로 묶여 생성되며, 이 블록들은 선형으로 연결되어 변경이 불가능한 구조를 이룬다. 모든 참여자는 동일한 거래 기록을 보유함으로써 데이터의 투명성과 무결성을 확보할 수 있으며, 중앙 기관 없이도 시스템의 신뢰성과 운영이 가능하다.

블록체인의 주요 특징은 다음과 같다.  
첫째, 탈중앙화(Decentralization)로 인해 특정 기관이나 개인이 시스템을 독점적으로 통제할 수 없다.  
둘째, 불변성(Immutability)을 통해 한 번 기록된 데이터는 수정이나 삭제가 불가능하다.  
셋째, 투명성(Transparency)을 기반으로 거래 기록이 네트워크 참여자 전체에게 공개된다.

이러한 특징은 금융, 물류, 의료 등 다양한 분야에서 블록체인의 활용 가능성을 높이고 있으며, 특히 P2P 송금 시스템 구축에 있어 신뢰성 확보에 큰 기여를 한다.

**2.2 스마트컨트랙트 개념 및 활용**

스마트컨트랙트(Smart Contract)는 블록체인 상에 저장되어 자동으로 실행되는 프로그램이다. 특정 조건이 충족되었을 때 미리 정해진 명령이 자동으로 실행되도록 설계되며, 이를 통해 신뢰성 있는 거래 및 계약 이행을 보장할 수 있다. 스마트컨트랙트는 주로 Ethereum과 같은 퍼블릭 블록체인 플랫폼에서 활용되며, Solidity 언어를 사용하여 작성된다.

스마트컨트랙트는 제3자 중개 없이 계약 당사자 간 직접적인 거래를 가능하게 하며, 수수료 절감 및 거래 속도 향상이라는 이점을 제공한다. 다만, 스마트컨트랙트는 배포 이후 수정이 어렵고, 코드 상의 오류나 보안 취약점이 심각한 결과를 초래할 수 있기 때문에, 설계 및 구현 단계에서 높은 수준의 주의가 요구된다.

본 연구에서는 스마트컨트랙트를 이용하여 송금 기능을 구현하고, 재진입 공격 방지(Reentrancy Attack Prevention) 기능을 추가하여 보안성을 강화하였다.

**2.3 기존 P2P 결제 시스템과 블록체인 기반 시스템의 비교**

기존의 P2P 결제 시스템은 PayPal, Venmo 등 중앙화된 플랫폼을 통해 사용자 간 송금을 지원한다. 이러한 시스템은 사용자 편의성 및 거래 속도 측면에서 장점을 가지나, 중개 기관의 서버 장애, 수수료 부담, 개인정보 노출 위험 등 여러 한계를 지닌다.

반면, 블록체인 기반 P2P 송금 시스템은 중앙 기관을 거치지 않고 거래가 이루어지므로, 다음과 같은 장점을 가진다.

* 거래 투명성 및 추적 가능성
* 중개 수수료 절감
* 시스템 장애 리스크 감소
* 사용자 개인정보 보호 강화

하지만 블록체인 시스템은 확장성 문제, 높은 트랜잭션 수수료(Gas Fee), 스마트컨트랙트 취약성 등 여전히 극복해야 할 기술적 과제를 안고 있다.

본 논문에서는 이러한 양 시스템의 장단점을 고려하여, 블록체인 기반 송금 시스템의 구현 가능성과 실용성을 검토하고자 한다.

**3. P2P 블록체인 송금 시스템 설계**

**3.1 시스템 아키텍처**

본 연구에서 설계한 P2P 송금 시스템은 스마트컨트랙트(P2PRemittance)를 중심으로 하여, 사용자 간 직접적인 입금 및 송금을 지원하는 구조로 구성된다. 사용자는 Ethereum 네트워크 상에서 개인 지갑을 통해 스마트컨트랙트와 상호작용하며, 모든 거래 기록은 블록체인에 저장된다.

**시스템 구성요소는 다음과 같다.**

* **사용자 계정 (Ethereum 지갑 주소):** 송금 및 입금 주체
* **P2PRemittance 스마트컨트랙트:** 잔액 관리, 송금 기능, 보안 기능 담당
* **Ethereum 블록체인:** 거래 기록 저장 및 스마트컨트랙트 실행 기반
* **프론트엔드 인터페이스 (선택적 구현):** 사용자 송금 요청 전송 (Metamask 등과 연동 가능)

**[그림 3.1] 시스템 아키텍처 다이어그램 (추후 삽입 예정)**

*(※ 추후 Word 작업 시 이 부분에 시스템 구성도를 삽입할 예정입니다.)*

**3.2 스마트컨트랙트 설계 및 기능 설명**

P2PRemittance 스마트컨트랙트는 다음과 같은 핵심 기능을 구현한다.

**3.2.1 입금 기능 (deposit)**

사용자는 스마트컨트랙트에 이더(ETH)를 입금할 수 있다. 입금 시, 입금자 지갑 주소와 입금 금액이 매핑되어 저장된다. 이 과정은 스마트컨트랙트 내 상태 변수인 balances를 통해 관리된다.

solidity

복사편집

function deposit() external payable {

balances[msg.sender] += msg.value;

}

**3.2.2 송금 기능 (transfer)**

입금된 잔액을 이용하여 다른 사용자에게 송금을 수행할 수 있다. 송금 시 송금자의 잔액은 감소하고, 수신자의 잔액은 증가한다. 송금 금액이 송금자의 잔액을 초과할 경우 트랜잭션은 실패한다.

solidity

복사편집

function transfer(address recipient, uint256 amount) external {

require(balances[msg.sender] >= amount, "Insufficient balance");

balances[msg.sender] -= amount;

balances[recipient] += amount;

}

**3.2.3 잔액 조회 기능 (getBalance)**

사용자는 본인의 스마트컨트랙트 상 잔액을 조회할 수 있다.

solidity

복사편집

function getBalance(address account) external view returns (uint256) {

return balances[account];

}

**3.2.4 재진입 공격 방어**

스마트컨트랙트의 보안성을 강화하기 위해, 재진입 공격(Reentrancy Attack) 방지 장치가 적용되었다. OpenZeppelin 라이브러리의 ReentrancyGuard를 상속받아, 외부 호출이 포함된 함수들에 대해 nonReentrant modifier를 적용하였다.

solidity

복사편집

function transfer(address recipient, uint256 amount) external nonReentrant {

require(balances[msg.sender] >= amount, "Insufficient balance");

balances[msg.sender] -= amount;

balances[recipient] += amount;

}

이를 통해 악의적인 반복 호출로 인한 잔액 탈취 공격을 효과적으로 차단하였다.

**3.3 송금 프로세스 흐름도**

본 시스템에서 사용자가 송금을 수행하는 과정은 다음과 같은 단계로 이루어진다.

1. 송금자는 스마트컨트랙트에 ETH를 입금한다.
2. 송금자는 수신자 주소와 송금 금액을 지정하여 송금 요청을 전송한다.
3. 스마트컨트랙트는 잔액 검증 후 송금자의 잔액을 차감하고 수신자의 잔액을 증가시킨다.
4. 모든 트랜잭션 기록은 블록체인에 영구 저장된다.

**[그림 3.2] 송금 프로세스 흐름도 (추후 삽입 예정)**

**4. 구현 및 실험 결과**

**4.1 개발 환경 및 기술 스택**

본 연구에서는 스마트컨트랙트 개발 및 테스트를 위해 다음과 같은 개발 환경과 기술 스택을 사용하였다.

* **개발 언어:** Solidity 0.8.28
* **개발 프레임워크:** Hardhat 2.23.0
* **블록체인 라이브러리:** Ethers.js 6.13.7
* **스마트컨트랙트 보안 라이브러리:** OpenZeppelin Contracts 4.9.3
* **Node.js 버전:** 20.16.0
* **테스트 네트워크:** Hardhat Localhost Node (127.0.0.1:8545)
* **IDE 및 에디터:** Visual Studio Code

모든 개발 및 테스트는 로컬 환경에서 이루어졌으며, 테스트를 위해 Hardhat에서 제공하는 가상의 Ethereum 네트워크를 활용하였다.

**4.2 주요 코드 설명**

**4.2.1 스마트컨트랙트 주요 구현**

P2PRemittance 스마트컨트랙트의 핵심 코드는 입금, 송금, 잔액 조회 기능과 보안 강화를 위한 재진입 공격 방지 로직을 포함하고 있다. 주요 기능별 코드는 앞서 제시한 바와 같다.

특히, 송금 기능에는 nonReentrant 제어자를 적용하여 외부 호출로 인한 반복 트랜잭션 실행을 차단하였다.

**4.2.2 배포 및 상호작용 스크립트**

스마트컨트랙트 배포와 테스트를 위해 Hardhat 스크립트를 작성하였다.

* **배포 스크립트 (deploy.js):**  
  스마트컨트랙트를 컴파일하고, Hardhat 로컬 노드에 배포한다.
* **상호작용 스크립트 (interact.js):**  
  배포된 컨트랙트에 연결하여 입금 및 송금 기능을 수동으로 테스트한다. 송금 후 송신자와 수신자의 잔액 변화를 확인한다.

이러한 스크립트를 통해 반복적인 테스트 절차를 자동화하고, 실험 결과를 신속히 수집할 수 있었다.

**4.3 테스트넷에서의 송금 실험**

Hardhat Localhost Node 환경에서 수동 실험을 수행하였다.  
다음은 대표적인 실험 절차와 결과이다.

1. **입금 실험:**
   * 송금자는 스마트컨트랙트에 1 ETH를 입금하였다.
   * 입금 후 송금자의 스마트컨트랙트 내 잔액은 1 ETH로 확인되었다.
2. **송금 실험:**
   * 송금자는 수신자에게 0.5 ETH를 송금하였다.
   * 송금 완료 후 송금자의 잔액은 0.5 ETH, 수신자의 잔액은 0.5 ETH로 정확히 반영되었다.
3. **결과 확인:**
   * 수동으로 트랜잭션 로그 및 잔액 변화를 검증하였으며, 모두 예상한 결과와 일치하였다.

**[그림 4.1] 수동 실험 결과 캡처 (추후 삽입 예정)**  
*(※ Word 편집 시 관련 실험 캡처 삽입 예정입니다.)*

**4.4 자동화 테스트 및 결과 분석**

자동화된 테스트 코드를 작성하여 스마트컨트랙트 기능을 검증하였다. 주요 테스트 항목은 다음과 같다.

* **입금 및 송금 후 잔액 검증:** 사용자가 입금 후 송금할 경우, 송신자와 수신자의 잔액이 정확히 변동되는지 검증하였다.
* **잔액 초과 송금 실패 검증:** 송금 요청 금액이 송금자의 잔액을 초과할 경우, 트랜잭션이 실패하는지를 검증하였다.
* **재진입 공격 방어 기능 검증:** 스마트컨트랙트 함수 호출 시 재진입 공격이 차단되는지를 검증하였다.

자동화 테스트는 Hardhat을 이용하여 실행되었으며, 모든 테스트 케이스가 정상적으로 통과하였다.

**[그림 4.2] 자동화 테스트 결과 캡처 (추후 삽입 예정)**

테스트 결과, 스마트컨트랙트의 기능적 안정성과 보안성은 실험 목적에 부합하는 수준으로 검증되었다.

**5. 보안 및 성능 분석**

**5.1 이중 지불(Double Spending) 방지 기법 적용 여부**

이중 지불(Double Spending)이란 동일한 자금을 두 번 이상 사용하는 것을 의미하며, 전통적인 금융 시스템뿐만 아니라 블록체인 시스템에서도 심각한 보안 위협으로 간주된다. 본 연구에서 구현한 P2PRemittance 스마트컨트랙트는 이중 지불을 방지하기 위해 다음과 같은 메커니즘을 적용하였다.

첫째, 입금된 금액은 스마트컨트랙트 내 balances 매핑을 통해 개별 사용자별로 관리되며,  
송금 시 잔액 검증(require(balances[msg.sender] >= amount))을 수행하여 사용자가 보유한 금액 이상을 송금할 수 없도록 제한하였다.

둘째, 트랜잭션 처리 시 잔액 차감과 수신자 잔액 증가가 원자적(Atomic)으로 이루어지며, 중간에 상태 변조가 발생할 수 없도록 하였다.

이를 통해 이중 지불 시도가 발생할 경우, 스마트컨트랙트는 자동으로 트랜잭션을 거부하며, 시스템의 무결성과 신뢰성을 유지할 수 있다.

**5.2 재진입 공격(Reentrancy Attack) 방어 기법**

재진입 공격은 스마트컨트랙트의 외부 호출 시점에 공격자가 다시 원래 함수를 호출하여, 상태가 완전히 업데이트되기 전에 자금을 탈취하는 공격 기법이다. 이러한 공격은 Ethereum 기반 스마트컨트랙트에서 매우 치명적인 보안 취약점으로 작용할 수 있다.

본 연구에서는 재진입 공격을 방지하기 위해 OpenZeppelin 라이브러리의 ReentrancyGuard를 상속받고, 주요 함수에 nonReentrant modifier를 적용하였다.

이를 통해 함수 실행 도중 중복 호출이 발생하는 것을 원천적으로 차단하였으며, 트랜잭션의 무결성을 보장할 수 있었다.

스마트컨트랙트에서 재진입 공격 방지 로직은 다음과 같은 순서로 작동한다.

1. 함수가 호출되면 내부적으로 '진입 중' 상태로 플래그가 설정된다.
2. 함수 실행이 완료되기 전에는 동일 함수의 재호출이 불가능하다.
3. 함수 실행이 정상적으로 종료되면 플래그가 해제된다.

본 실험 결과, 재진입 공격을 시도하는 테스트 케이스를 추가하였으나, 모든 공격이 차단되어 안전성을 확인할 수 있었다.

**5.3 기존 금융 시스템과의 보안성 비교**

| **구분** | **기존 중앙화 금융 시스템** | **블록체인 기반 P2PRemittance 시스템** |
| --- | --- | --- |
| 보안 주체 | 중앙 서버, 관리자 | 네트워크 전체, 스마트컨트랙트 |
| 이중 지불 대응 | 중앙 기록 확인 | 스마트컨트랙트 내 자동 검증 |
| 시스템 장애 대응 | 중앙 서버 장애 시 전체 중단 위험 | 노드 다중 분산 저장으로 높은 가용성 |
| 개인정보 노출 위험 | 사용자 데이터 저장 및 관리 필요 | 최소한의 정보만 블록체인에 기록 |
| 재진입 공격 위험 | 해당 없음 | 방어 기법 적용 필요 (nonReentrant) |

본 시스템은 중앙 서버에 의존하지 않음으로써 시스템 장애에 대한 내성이 강하며, 자동화된 스마트컨트랙트 로직을 통해 이중 지불과 재진입 공격과 같은 주요 보안 위협을 효과적으로 방지할 수 있다. 반면, 스마트컨트랙트 자체의 설계 오류에 대한 위험성은 여전히 존재하기 때문에, 코드 검증 및 보안성 강화는 필수적이다.

**6. 한계점 및 개선 방안**

**6.1 한계점**

본 연구를 통해 개발된 P2PRemittance 스마트컨트랙트는 블록체인 기반 P2P 송금 시스템의 기본 기능을 성공적으로 구현하고 보안성을 검증하였다. 그러나 다음과 같은 한계점을 지닌다.

**6.1.1 기능적 제한**

본 시스템은 입금, 송금, 잔액 조회라는 기본 기능만을 제공하며, 송금 요청 취소, 환불, 수수료 설정 등의 부가 기능은 구현되어 있지 않다. 실제 금융 환경에서는 다양한 예외 상황에 대한 처리가 요구되므로, 기능적 확장성이 필요하다.

**6.1.2 사용자 인터페이스 부재**

현재 구현된 시스템은 콘솔 기반 상호작용에 의존하고 있으며, 사용자가 직접 송금 요청을 수행하기 위해 명령어를 입력해야 한다. 이는 블록체인 기술에 익숙하지 않은 일반 사용자에게는 진입 장벽이 될 수 있다.

**6.1.3 가스비(Gas Fee) 및 성능 최적화 미흡**

스마트컨트랙트 실행 시 발생하는 가스비 최적화는 충분히 고려되지 않았다. 송금 과정에서 발생하는 트랜잭션 비용이 높을 경우, 실제 서비스화에 있어 사용자 경험을 저해할 수 있다.

**6.1.4 테스트 환경의 제한**

본 실험은 Hardhat Localhost Node 상에서만 수행되었으며, 실제 퍼블릭 테스트넷(예: Goerli, Sepolia)이나 메인넷 배포를 통한 실험은 진행되지 않았다. 따라서 네트워크 지연, 블록 혼잡도 등의 현실적 요소를 고려한 성능 검증이 이루어지지 않았다.

**6.2 개선 방안**

이러한 한계점을 보완하기 위해 다음과 같은 개선 방안을 제시한다.

**6.2.1 기능 확장**

송금 요청 취소 기능, 송금 수수료 부과 기능, 거래 내역 조회 기능 등을 추가함으로써, 실제 금융 서비스에 적합한 송금 시스템으로 확장할 수 있다. 또한, 다중 서명(Multisig) 기능을 추가하여 보안성을 강화하는 방법도 고려할 수 있다.

**6.2.2 사용자 친화적 인터페이스 개발**

Web3.js 또는 Ethers.js를 활용하여 웹 기반 사용자 인터페이스를 개발하고, Metamask와 연동하여 송금 과정을 직관적으로 수행할 수 있도록 지원할 수 있다. 이를 통해 사용자 접근성과 편의성을 크게 향상시킬 수 있다.

**6.2.3 가스비 최적화**

트랜잭션 처리 로직을 최적화하고, 불필요한 상태 변수 접근을 줄임으로써 가스비를 절감할 수 있다. 또한, Solidity 최적화 기법(예: calldata 사용, 가스 절약 패턴 적용)을 적극 도입하는 것이 필요하다.

**6.2.4 테스트넷 및 메인넷 배포 실험**

향후 연구에서는 Goerli 또는 Sepolia 테스트넷에 스마트컨트랙트를 배포하고, 실제 네트워크 환경에서 송금 실험을 수행하여 블록체인 혼잡 상황, 트랜잭션 승인 지연 시간 등을 고려한 현실적인 성능 평가를 진행할 예정이다.

**7. 결론 및 향후 연구 방향**

**7.1 연구 결과 요약**

본 논문에서는 블록체인 기술을 기반으로 한 P2P 송금 시스템을 설계하고, 이를 구현 및 검증하였다.  
스마트컨트랙트인 P2PRemittance를 개발하여 사용자의 이더(ETH) 입금, 송금, 잔액 조회 기능을 지원하고, 재진입 공격 방어 및 이중 지불 방지 기법을 적용하여 보안성을 강화하였다.

로컬 개발 환경인 Hardhat Node를 활용하여 수동 실험 및 자동화 테스트를 수행하였으며, 그 결과 스마트컨트랙트의 기능적 안정성과 보안성이 요구 수준에 부합함을 확인하였다. 입금 및 송금 기능은 정확하게 동작하였고, 잔액 초과 송금이나 재진입 공격에 대한 방어도 정상적으로 작동하였다.

또한, 기존 중앙화 금융 시스템과 비교하여, 블록체인 기반 시스템의 탈중앙화, 무결성, 보안성 측면에서의 장점을 확인할 수 있었다. 다만, 기능적 제한, 사용자 접근성 문제, 가스비 최적화 부족 등 몇 가지 한계점도 발견되었으며, 이에 대한 개선 방향을 제시하였다.

**7.2 향후 발전 가능성**

향후 연구에서는 다음과 같은 확장 및 고도화 방향을 고려할 수 있다.

첫째, 스마트컨트랙트 기능을 다각화하여, 송금 취소, 환불, 거래 기록 조회, 다중 서명 기반 승인 등 보다 복합적인 금융 서비스 기능을 추가할 예정이다.

둘째, 사용자 편의성을 높이기 위해 Web 기반 사용자 인터페이스를 개발하고, Metamask와 연동하여 비개발자도 손쉽게 사용할 수 있는 환경을 구축할 계획이다.

셋째, 퍼블릭 테스트넷 및 메인넷 상에서 실거래 실험을 진행함으로써, 실제 네트워크 환경에서의 성능과 안정성을 종합적으로 평가할 필요가 있다.

넷째, 스마트컨트랙트 코드의 보안성을 더욱 강화하기 위해 서드파티 보안 감사(Security Audit)를 수행하고, 가스비 최적화 및 코드 최적화 기법을 적용하여 비용 효율성과 처리 속도를 향상시킬 것이다.

본 연구를 토대로 블록체인 기반 P2P 송금 시스템의 실용적 가능성을 제시할 수 있었으며, 향후 추가적인 연구와 개발을 통해 실질적인 상용화 가능성도 충분히 기대할 수 있다.