스마트 컨트랙트(smart contract)

https://youtu.be/u6kP8twZ1us

한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB

스마트 컨트랙트

이더리움 스마트 컨트랙트

스마트 컨트랙트의 문제점

스마트 컨트랙트

스마트 컨트랙트

스마트 컨트랙트는 중간에 제3의 보증기관을 끼우지 않고 개인간(P2P)에 원하는 계약을 체결할 수 있도록 해주는 디지털 전자계약 기능이다.

표 1 서면 계약서와 스마트 컨트랙트의 차이

	서면 계약서	스마트 컨트랙트
작성 언어	자연어	컴퓨터 코드
명확성	조건에 따른 계약 이행 내용이 이해자의 해석에 따라 달라짐	조건에 따른 계약 수행 내용이 명확
이해자	사람	컴퓨터
계약 수행 방안	사람 및 사법기관에 의한 법리적 수행	신뢰 네트워크에서 조건 갱신에 따른 계약 자동 이행

비탈릭 부테린(Vitalik Buterin)은 스마트 계약 플랫폼인 이더리움을 개발할 것을 제안하고, 2015년 7월 30일 이더리움 개발에 성공하여 실제 서비스를 시작했다.

솔리디티(solidity)라는 프로그래밍 언어를 사용하여, 계약 기간, 금액, 조건 등을 미리 코딩해 두면 어떠한 종류의 계약도 자동 실행되도록 만들 수 있다.

이더리움 스마트 컨트랙트

이더리움 스마트 컨트랙트

스마트 컨트랙트를 구현하기 위한 컨트랙트 코드는
이더리움 가상머신이라는 독립된 실행환경에서 실행된다.

여기에 스마트 컨트랙트를 실행할 때마다 **수수료**인 **가스(gas)**를 발생시키고
네트워크상에 수수료의 한계를 설정하여 무한루프를 막았다.

무한히 반복되는 조건을 만들어 스마트 컨트랙트를 실행시키면 중간에 수수료 한계점에 도달하게 되는데, 이때 중단된다.

이때 솔리디티(Solidity) 언어로 프로그래밍 된다. 솔리디티 언어로 된 스마트 컨트랙트는 컴파일러(solc)에 의해 바이트코드로 컴파일되고, 컴파일된 바이트 코드는 블록에 포함되어, 이더리움 가상머신에 의해 실행된다.

이더리움 스마트 컨트랙트 작동 원리

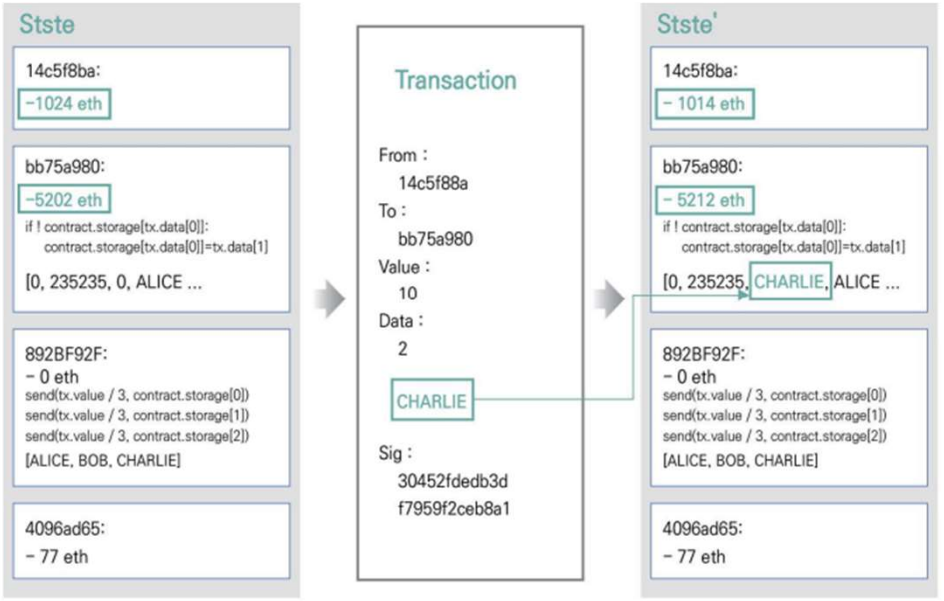
작동원리

블록체인 기반 스마트 컨트랙트는 기본적으로 모든 트랜잭션 **로그**가 저장된
블록체인 데이터베이스와 스마트 컨트랙트의 상태를 저장하는 데이터베이스 두 가지가 존재한다.

여기서의 스마트 컨트랙트는 상태를 변경할 수 있는
애플리케이션이라고 할 수 있고, 스마트 컨트랙트의
상태는 해당 애플리케이션에서 사용하는 변수라고
할 수 있으며, 이를 변경하기 위한 입력값은
트랜잭션에 포함되어 있다.

스마트 컨트랙트는 모든 데이터를 서로 공유하기 때문에
특정한 사용자가 스마트 컨트랙트의
실행 결과를 조작하려 해도 조작할 수 없다.

블록체인이 모든 트랜잭션의 무결성을 보장해 주는 방식으로
스마트 컨트랙트의 무결성도 보장할 수 있다.



스마트 컨트랙트의 문제점

기술적 문제점

- 한번 배포되어 블록으로 생성된 스마트 계약은 수정이 불가능하기 때문에, 업그레이드나 버그 패치, 보안 취약점 수정 등이 어렵다. 최근 들어 업그레이드 가능한 스마트 계약 작성 방법이 활발히 연구되고 있으나, 플랫폼 차원에서 해결된 문제라고 보기는 힘들다.

- 솔리디티(Solidity) 언어가 비교적 최근에 개발된 언어이고 그렇게 빠르게 업그레이드되지 않고 있어서, 타 개발 언어에서 기본적으로 지원되는 타입이나 연산자 또는 명령어가 부족하다.

정책적 문제점

- 비싼 가스 수수료 문제
- 다자간 스마트 계약 문제
- 오라클 문제

Q & A