블록체인 기반 스마트 컨트랙트 활용 사례 연구

김종협(더루프 대표)

요 약

스마트 컨트랙트(Smart Contract)란 디지털로 작성된 계약서를 의미한다. 스마트 컨트랙트 기술은 디지털의 특성상 서면으로 기술된 계약서에 비해 명확성을 가지고 있으며 조건에 따라 디지털로 자동 수행이 가능하다는 장점이 있다. 이러한 스마트 컨트랙트 기술은 무결성 보장 및 조작이 불가능한 기술인 블록체인(Blockchain)을 통해 이더리움(Ethereum)에서 쉽게 사용할 수 있도록 구현되었다. 블록체인 기반 스마트 컨트랙트 기술은 그 실행 내용의 무결성과 조작되지 않음을 보장하여 스마트 컨트랙트로 계약을 체결하고 계약 조건에 따라 자동으로 계약을 이행할 수 있도록 보장한다.

블록체인 기반 스마트 컨트랙트는 디지털로 계약을 수행할 수 있다는 장점과 계약이 조건대로 실행된다는 보장, 실제 블록체인의 암호화화폐(cryptocurrency)를 계약을 통해 이동할 수 있다는 장점 때문에 금융권을 중심으로 다양한 연구와 투자가 확대되고 있다.

본 제언에서는 블록체인 기반 스마트 컨트랙트 기술에 대한 역사와 그 동작 방식, 블록체인 별 스마트 컨트랙트 구현 방식 등을 알아보고 이러한 스마트 컨트랙트의 활용 사례를 알아보고자 한다.

01 블록체인 기반 스마트 컨트랙트 활용 사례 연구

I 서 론

디지털 상에서 데이터 무결성 보장과 조작방지를 제공하여 디지털 데이터에 신뢰를 줄 수 있는 블록체인 기술이 부상하면서 블록체인을 단순한 거래 저장 시스템에서 벗어나 다양한 도메인으로 확장할 수 있게 해주는 기술인 스마트 컨트랙트 기술 또한 주목받고 있다.

스마트 컨트랙트 기술은 Nick Szabo가 1994년에 처음 제안한 거래 프로토콜로서 2015년 스마트 컨트랙트 전문 블록체인인 이더리움의 등장과 함께 주목받게 되었다. 스마트 컨트랙트는 조건에 따라 계약이 디지털로 자동수행이 가능하다는 장점을 가지고 있으며 여러 다양한 서비스에 활용할 수 있다. 예를 들어 스마트 컨트랙트를 통해 기존의 가상화폐 거래에만 활용되던 블록체인을 토큰으로 발행하거나 에스크로 서비스, 인증서비스 등 다양한 서비스에도 활용할 수 있게 되었다.

본고에서는 '블록체인 기반 스마트 컨트랙트 활용 사례 연구'에 대해 다음과 같은 순서로 살펴보고자 한다. 우선 스마트 컨트랙트의 역사와 개념, 동향에 대해 알아봄으로써 기본적인 이해를 돕도록 한다. 그 후 블록체인 별 스마트 컨트랙트의 특징과 내부 구성에 대해 살펴보고, DAO, 금융투자 업권 사업 등 실제 스마트 컨트랙트를 서비스에 활용한 사례에 대해 살펴보고자한다.

Ⅱ 스마트 컨트랙트 소개

1. 스마트 컨트랙트의 역사

스마트 컨트랙트는 Nick Szabo가 1994년에 제안한 컴퓨터 트랜잭션 프로토콜이다. 스마트 컨트랙트의 목표는 지불 조건, 유치권, 기밀 유지 및 시행과 같은 일반적인 계약 조건을 충족시키고 악의적이거나 우발적인 예외를 최소화하며 신뢰할 수 있는 중개인의 필요성을 최소화 하는 것이다.[1] 이를 위해 컴퓨터 코드로 스마트 컨트랙트를 생성하고 조건에 따라 자동으로 계약을 이행하게 한다. 컴퓨터 코드로 스마트 컨트랙트를 작성할 경우, 기존 서면으로 작성하는 계약에 비해 계약의 내용이 명확해지고 조건에 따른 즉각 이행이 가능하다. 그러나 디지털 상의 데이터는 쉽게 위변조가 가능하고 각 데이터의 무결성을 보장할 수 있는 기술이 부족했기 때문에 이러한 개념을 실제로 적용하기에는 많은 한계가 있었다.

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

그러나 2009년 최초의 암호화 화폐인 비트코인이 개발되고 비트코인의 신뢰성 보장 기술인 블록체인이 등장하자 스마트 컨트랙트가 다시 부상하기

1) Tapscott, Don; Tapscott, Alex (May 2016). The Blockchain Revolution: How the Technology Behind Bitcoin is Changing Money, Business, and the World. pp. 72, 83, 101, 127. ISBN 978-0670069972.

시작했다. 블록체인은 해시 연결과 합의 알고리즘을 통하여 P2P 네트워크에 참가하는 모든 노드들이 같은 데이터를 공유하게 하여 데이터의 신뢰성과 무결성을 보장하는 기술이다. 이러한 블록체인 기술을 바탕으로 스마트 컨트랙트를 구성하면 다양한 계약을 디지털 상에서 할 수 있을 것이라는 기대를 모았고, 이더리움과 같은 스마트 컨트랙트를 지원하는 블록체인 플랫폼들이 개발되게 되었다.

2. 블록체인 기반 스마트 컨트랙트

기존 디지털 프로토콜의 낮은 신뢰성과 언제나 복제 및 위변조가 가능하다는 문제 때문에 실제 구현되기 어려웠던 스마트 컨트랙트는 블록체인 기술을 통해 무결성을 보장하고 조작방지가 가능한 블록체인 기반 스마트 컨트랙트로 개발될 수 있게 되었다.

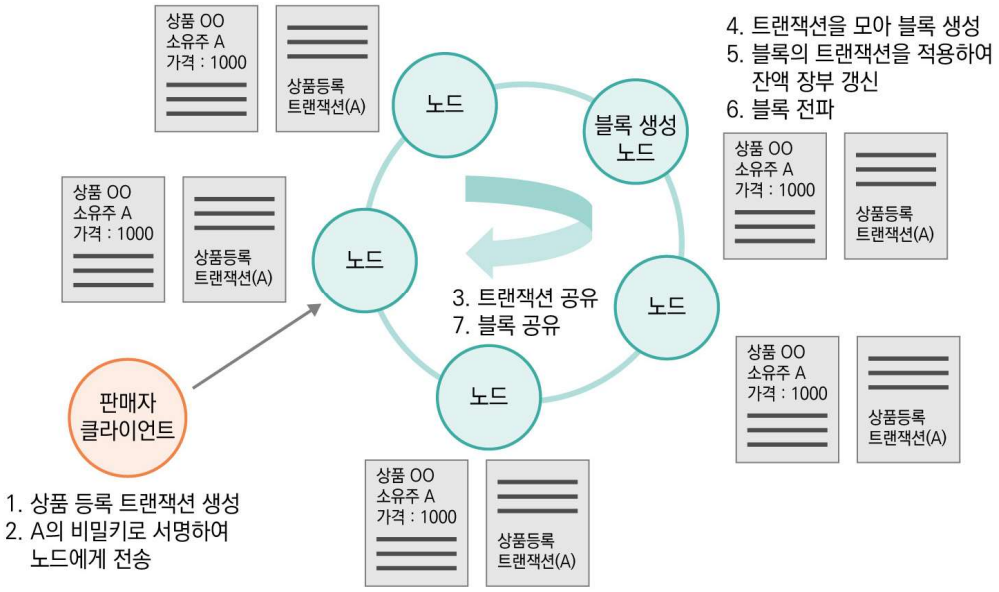
블록체인 기반 스마트 컨트랙트는 기존 거래의 무결성만 보장하던 블록체인 시스템의 한계를 넘어 조건과 상황에 따라 자동으로 계약 내용을 이행하는 스마트 컨트랙트 시스템으로 진화하였다. 이러한 블록체인 기반 스마트 컨트랙트를 이용하여 기존 블록체인 시스템에서는 구현하기 어려운 토큰 발행, 주식 발행, 인증 서비스, 보험 청구 서비스와 같은 다양한 서비스들이 테스트되고 개발·연구되기 시작하였다.

스마트 컨트랙트의 동작 방식은 스마트 컨트랙트를 운영하는 블록체인의 특성과 운영 전략에 따라 실행 방법이 다양하지만 대략적인 실행 방식은 유사하다. 본 장에서는 스마트 컨트랙트를 이용해 상품을 판매하려는 판매자가 스마트 컨트랙트에 상품을 올리는 예제를 통하여 블록체인 기반 스마트 컨트랙트의 동작 방식에 대해 설명하려고 한다.

블록체인 기반 스마트 컨트랙트는 기본적으로 모든 트랜잭션 로그가 있는 블록체인 데이터베이스와 스마트 컨트랙트의 상태(State)[2]를 저장하는

데이터베이스 두 가지가 존재한다. 스마트 컨트랙트의 상태를 저장하는 데이터베이스는 그 구현체마다 차이가 존재한다. 이더리움과 같은 경우 페트리샤 머클 트리(Patricia Merkle Tree)[3]를 블록체인에 같이 포함하였으며, IBM Fabric이나 JP Morgan의 Kadena같은 블록체인의 경우 별도의 블록체인 데이터베이스와 스마트 컨트랙트 데이터베이스를 완전히 분리하여 사용한다.

그림 1 스마트 컨트랙트 동작 예제



[그림 1]은 블록체인 기반 스마트 컨트랙트의 동작 과정을 그림으로 보여주는 예제이다. 그림에서 노드의 데이터베이스(사각형 다이어그램) 중 왼쪽에 있는 데이터베이스는 스마트 컨트랙트의 상태를 나타내고 오른쪽에 있는 데이터베이스는 블록체인 데이터베이스를 나타내고 있다. 생성자가 상품을 올리겠다는

2) 상태는 현재의 스마트 컨트랙트 실행 상태를 의미하며 단순한 가상화폐 거래를 위한 스마트 컨트랙트에서는 거래 참여자의 가상화폐 잔고가 상태에 해당하며 복잡한 스마트 컨트랙트에서는 계약과 관련된 다양한 변수 및 데이터가 상태에 해당

3) 이더리움 페트리샤 머클 트리 : https://github.com/ethereum/wiki/wiki/Patricia-Tree

트랜잭션을 만들어 블록체인에 전송하면 (1~2) 블록체인의 노드들은 해당 트랜잭션을 공유한다. (3) 블록체인 내부의 합의 알고리즘에 의해 선택된 블록 생성 노드가 해당 트랜잭션을 포함해 블록을 생성하고 블록을 브로드캐스팅한다. (4~6) 블록을 전달 받은 각 노드는 블록을 자신의 블록체인에 추가하고 해당 블록에 저장되어 있는 트랜잭션을 적용시켜 자신의 스마트 컨트랙트 데이터베이스를 갱신시킨다. 이러한 과정을 통해 모든 블록체인의 노드들이 같은 스마트 컨트랙트 상태 데이터베이스를 공유하게 된다.

블록체인 기반 스마트 컨트랙트는 위의 기술한 방식을 통하여 모든 데이터를 공유하기 때문에 특정한 사람이 스마트 컨트랙트의 실행 결과를 조작하려해도 조작할 수 없으며 블록체인이 모든 트랜잭션의 무결성을 보장해 주는 방식으로 스마트 컨트랙트의 무결성도 보장할 수 있다. 이러한 블록체인 기반 스마트 컨트랙트는 블록체인의 가장 핵심적인 특징으로 여겨지며 이더리움 이후의 대부분의 새로운 블록체인은 스마트 컨트랙트 기능을 기본적으로 탑재한다.[4)]

또한 스마트 컨트랙트는 이더리움과 같은 공개 블록체인(Public Blockchain)뿐 아니라 사설 블록체인(Private Blockchain) 쪽에서도 활발하게 연구 중이다. 사설 블록체인은 비트코인, 이더리움과 같이 누구나 참여할 수 있는 블록체인이 아닌 제한된 참여자만 참가할 수 있는 블록체인이다. 블록체인에 참여 가능한 기관을 제한할 경우 사설 블록체인은 기관 사이에 신뢰를 구축해주어 비신뢰 기관 간 공동 서비스 혹은 신뢰 업무를 수행할 수 있게 해준다. 사설 블록체인은 그 특성상 내부 화폐가 없는 경우가 많고 기존 서비스 인프라를 대체하는 기능이 크기 때문에 대체로 서비스 로직이 복잡하다. 때문에 거의 모든 사설 블록체인은 스마트 컨트랙트를 기본으로 탑재한다. 공개 블록체인은 토큰 발행이 가장 많이 사용하는 스마트 컨트랙트인 반면 사설 블록체인 스마트 컨트랙트는 청산 업무, 인증 서비스, 복잡한 비즈니스 로직 통합 등에 이용한다.

4) Stratis, Golem, IBM Fabric, R3 Corda, Tendermint 등

3. 스마트 컨트랙트 기술 동향

블록체인 기반의 스마트 컨트랙트 기술은 2015년 이더리움을 통해 처음 개발된 이후 여러 블록체인 플랫폼을 통하여 다양한 스마트 컨트랙트가 개발되었다. 초창기 스마트 컨트랙트 분야에서 가장 이슈가 되었고 향후 해킹 사건으로 인해 더욱 이슈가 되었던 스마트 컨트랙트는 The DAO(Decentralized Autonomous Organization)이다. DAO는 블록체인 상의 스마트 컨트랙트 기술로 구현한 탈중앙화된 자율 조직으로서 중앙의 운영 주체 없이 개인들이 자율적으로 제안 및 투표를 하여 다수결로 의결하여 운영되는 조직이다.

DAO는 운영 권리를 DAO토큰이라는 이더리움 상의 스마트 컨트랙트로 구매할 수 있게 하였고 DAO토큰을 보유한 주주들이 운영 방안을 함께 결정하도록 하였다. 이러한 방식으로 최초의 탈 국가적 분산 자율 조직을 구성하였으나 DAO 스마트 컨트랙트 코드의 취약점[5]을 발견한 해커가 DAO 스마트 컨트랙트에 DAO토큰만큼 보관 되어있던 암호 화폐를 도난하는 사건이 발생하였다. DAO의 부흥과 쇠퇴는 이더리움 커뮤니티와 이더리움 암호화 화폐 가격에 큰 영향을 미쳤다. DAO의 부흥으로 기존 한화로 1만원 초반 가격을 형성하던 이더리움의 가격이 2만원 중반 가격까지 치솟았고 DAO해킹과 함께 1만원 이하로 하락하였다.

DAO해킹은 스마트 컨트랙트 코드 취약점을 통해 해킹당한 것으로 이더리움 블록체인 자체가 해킹당한 것은 아니었다. 해당 사건으로 인해 이더리움 위에 스마트 컨트랙트가 생성되면 안전하다는 생각이 깨지게 되었으며 스마트 컨트랙트 코드의 취약점을 보완하기 위하여 스마트 컨트랙트 코드 '정적 분석' 솔루션이 생겨나기 시작했으며 스마트 컨트랙트가 안전한지 검증해주는 검증 업체도 이 당시부터 생겨났다. 이때 DAO로 손실이 큰

5) DAO Contract안의 Split함수를 이용하여 사용자의 Contract에 가상화폐를 출금했을 때 출금 내역이 Contract에 즉시 반영되지 않아 Split함수를 계속 호출하여 원래 출금되어야 할 금액보다 더 많은 금액을 출금할 수 있는 취약점

유저들에게 보상을 주기 위해 이더리움은 하드포크(Hardfork)[6]를 수행한다.

DAO의 해킹 사태에도 불구하고 많은 이용자들이 이더리움의 스마트 컨트랙트를 이용하여 다양한 토큰을 발행하였고, 스마트 컨트랙트 기반의 이더리움은 여전히 가장 큰 영향을 미치는 스마트 컨트랙트 서비스이다. Augur(예측시장 서비스) 토큰, DICE(겜블링) 토큰 등 다양한 토큰이 이더리움 네트워크에 올라갔다. 또한 이더리움 내부에 있는 서비스에 대한 토큰 뿐 아니라 새로운 블록체인 기반 가상 화폐 생성에 대한 보증을 하는 ICO[7] 또한 대부분 이더리움 스마트 컨트랙트를 통해 이루어진다.

대부분의 사설 블록체인은 가상화폐를 이용할 필요가 없어 토큰 판매가 아닌 블록체인을 통한 새로운 신뢰 서비스를 스마트 컨트랙트로 구현하고 있다. 블록체인 스마트 컨트랙트를 이용하여 기존에 믿지 못하던 기관과의 자동화된 거래를 수행하던가, 기존 비 신뢰 시스템 간의 통신에서 발생하는 낭비를 해결하고, 법률적 처리로 많은 시간이 걸리는 과정을 스마트 컨트랙트로 수행하게 하여 단순화하는 등 다양한 서비스를 구현하려 하고 있다. 그러나 사설 블록체인 기술은 금융 등의 제도권에서는 아직 본격적인 상용화 단계가 아닌 시험 단계가 대부분으로 다양한 서비스의 PoC를 수행 중이다.

대표적으로 IBM은 기존 해양 물류 수출입의 복잡한 과정을 블록체인 기반 스마트 컨트랙트 서비스를 통해 단순화 하려는 시도를 하고 있으며, R3는 다양한 화폐의 환거래를 스마트 컨트랙트를 통해 환률을 결정하고 거래를 자동화 하는 서비스를 개발 중이다. theloop는 스마트 컨트랙트를 통해 인증서를 발급하고 갱신하고 폐기하는 인증 서비스와, 복잡한 보험 청구 프로세스를 단순화하는 보험금 자동 청구 서비스, 파생상품을 공시하고 거래하는 파생상품 거래 서비스를 개발하고 있다.

---

6) 블록체인의 문제를 해결하기 위하여 해커가 공격한 트랜잭션 및 적용내용을 빼고 다시 블록을 생성하여 블록체인 내역을 바꾸는 과정. 거래소와 마이닝 풀들 간의 합의가 필요

7) Initial Coin Offering : 추후 나올 화폐에 대한 권한을 다른 가상화폐로 구매하는 것

Ⅲ 스마트 컨트랙트 기술 해부

1. 이더리움 스마트 컨트랙트

이더리움은 최초의 블록체인 기반 스마트 컨트랙트 플랫폼으로 가장 많은 스마트 컨트랙트가 동작하는 플랫폼이다. 이더리움은 공개 블록체인으로써 '이더(Ether)'라는 가상 화폐를 기반으로 스마트 컨트랙트를 동작할 수 있도록 설계되었다.

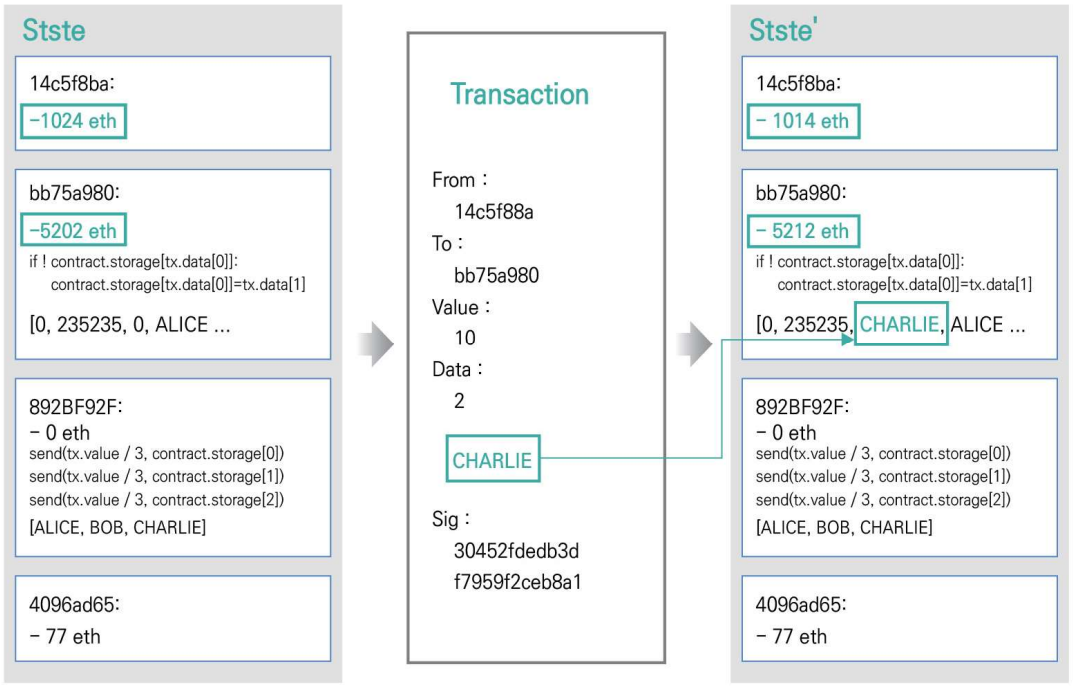
이더리움의 스마트 컨트랙트는 공개형 블록체인 위에서 동작하기 때문에 비트코인처럼 모든 정보가 이더리움 내의 모든 노드에게 공유된다. 해당 이더리움 노드는 전 세계 적으로 30,000개 이상[8]이기 때문에 스마트 컨트랙트에 기입된 정보를 조작하는 것은 어려운 일이다. 하지만 이러한 정보 공유의 특징은 다양한 서비스를 스마트 컨트랙트로 작성하는데 문제가 되기도 한다. 개인정보와 같이 공유되지 말아야할 중요한 데이터를 이더리움의 스마트 컨트랙트에서 처리하는 것은 사실상 불가능하다.

이더리움의 블록에는 트랜잭션의 목록과 트랜잭션의 결과(계정별 이더 잔고, 스마트 컨트랙트의 경우 변수 및 데이터)인 상태가 기록되며 전체 노드에 공유된다. 상태는 계정(Account)들로 구성되며 계정은 외부소유(Externally Owned) 계정과 컨트랙트 계정으로 구분된다. 외부소유 계정에는 이더 잔고가 기록되고 컨트랙트 계정에는 추가로 스마트 컨트랙트 코드와 관련 데이터가 추가로 포함된다.

[그림 2]는 트랜잭션에 의해 이더리움의 상태가 변경되는 과정을 나타낸 것으로 계정 간에 이더가 이체(14c5f8ba에서 bb75a980으로 10이더 이체)되고 스마트 컨트랙트 코드에 의해 특정 데이터가 추가(bb75a980에 'CHARLIE' 추가)됨에 따라 상태가 변경된 것을 확인할 수 있다.

8) https://ethernodes.org/network/1

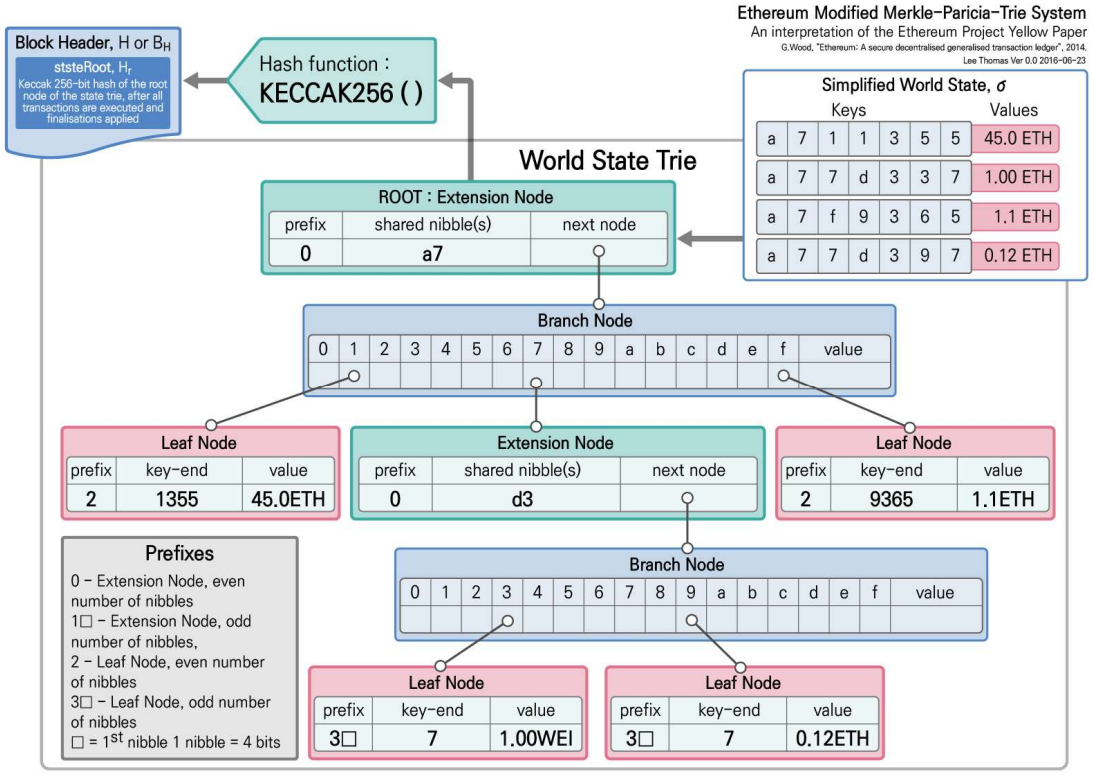
그림 2 이더리움 스마트 컨트랙트 상태 변경 예[9)]



이더리움에서는 상태 정보를 효과적으로 저장·관리하기 위해 페트리샤 머클 트리라는 자료구조를 이용한다. 기존 트리 자료구조의 너무 많은 노드가 생성되는 단점을 극복하기 위해 페트리샤 머클 트리는 중복되는 데이터를 하나의 노드로 묶은 구조이다. 실제로 [그림 3]과 같이 각 이더리움의 계정(Key)에 대한 정보(Value)가 트리형태로 저장되며 key값이 유사한 노드들을 묶어서 관리하는 것을 확인할 수 있다. 트랜잭션에 의해 변경된 각 계정의 내용이 페트리샤 머클 트리에 저장되며 스마트 컨트랙트 또한 계정의 형태로 이더리움 네트워크에 참여하기 때문에 트리에 저장·관리된다. 결국, 스마트 컨트랙트의 모든 상태(저장된 변수 및 데이터)변화는 페트리샤 머클 트리에 이력이 남아 추적이 가능하다. 또한 비트코인의 머클 트리처럼 트리에 리프 노드의 단방향 해시 데이터가 상위 노드에 저장되기 때문에 악의적인 누군가에 의한 상태 정보 조작을 쉽게 감지할 수 있다.

9) https://github.com/ethereum/wiki/wiki/%5BKorean%5D-White-Paper

그림 3 이더리움의 페트리샤 머클 트리 예[10)]



다양한 스마트 컨트랙트가 실행될 수 있으며 누구나 등록하고 사용할 수 있는 이더리움은 이더리움 네트워크를 멈추려는 악의적인 시도가 발생할 수 있다. 예를 들어, 스마트 컨트랙트는 프로그래밍 언어로 만들어져 있기 때문에 악의적으로 무한 루프를 발생시켜 네트워크에 서비스 거부 공격[11)]을 수행할 수 있다. 만약 무한 루프를 발생시키는 트랜잭션이 블록에 포함되어 네트워크에 전파될 경우 각 노드들은 블록을 검증하기 위해 해당 트랜잭션을 적용(실행)할 것이고 결국 무한 루프에 빠져 네트워크 전체가 멈출 수 있다. 이러한 문제를 해결하기 위하여 이더리움은 가스(Gas)라는 개념을 도입하였다. 가스는 스마트 컨트랙트 실행 시 발생하는 수수료로서 각 명령어 마다 요구되는 가스의 양이 정해져있다. 그리고 각 트랜잭션마다 사용할 수 있는 가스

10) ttps://ethereum.stackexchange.com/questions/6415/eli5-how-does-a-merkle-patricia-trie-tree-work
11) 시스템을 악의적으로 공격해 해당 시스템의 자원을 부족하게 하여 원래 의도된 용도로 사용하지 못하게 하는 공격

한계치가 정해져 있으며 의도적으로 명령어를 반복 실행시켜 네트워크를 느리게 하는데도 많은 수수료가 필요하기 때문에 무한 루프가 포함된 스마트 컨트랙트를 실행하는 것은 사실상 불가능하다.

그러나 이더리움의 스마트 컨트랙트에는 몇 가지 한계점이 존재한다. 먼저, 스마트 컨트랙트 중에 외부 서비스에서 데이터를 받아와 처리하는 것이 불가능하여[12] 이더리움 네트워크 외의 다른 데이터를 활용하는 스마트 컨트랙트를 개발하는 것이 어렵다. 그리고 데이터가 모든 참여자에게 공개되어 개인정보 등 민감한 데이터를 처리하는 서비스의 개발이 어렵다. 또한 실행 시 마다 수수료가 부과되기 때문에 복잡한 로직이 있는 서비스를 만들기 힘들다. 이러한 한계점으로 인해 다양한 서비스가 올라가지 못하고 이더리움의 스마트 컨트랙트는 이더를 통한 새로운 블록체인과 새로운 서비스의 토큰 발급 서비스 위주로 발전하였다.

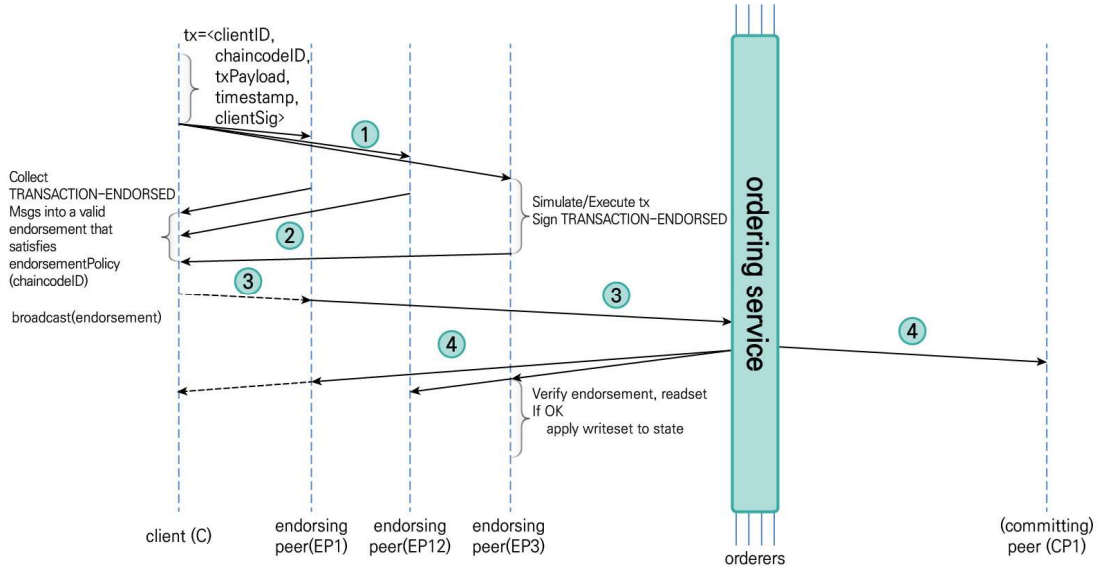
2. Hyperledger Fabric, R3 Corda 스마트 컨트랙트

Hyperledger Fabric과 R3 Corda는 대표적인 사설 블록체인 플랫폼이다. Hyperledger는 리눅스 재단에서 시작하여 세계 유수의 기업들이 공동으로 참여하고 있는 범 산업용 분산원장 표준화 프로젝트이다. 깃허브(Github)[13]를 통해 블록체인 관련 프로젝트들을 공개하고 있으며 Intel, IBM 등 국제적 기업들이 프로젝트에 참여하고 있다. Fabric은 Hyperledger 프로젝트 중 가장 활발하게 진행 중인 프로젝트로 IBM이 주도하고 있다.

Fabric은 모듈 아키텍처 기반의 블록체인 플랫폼으로서 합의알고리즘 등과 같은 블록체인의 기능을 추가 및 변경하기 용이하도록 설계되어 있다. Fabric도 스마트 컨트랙트를 지원하며 스마트 컨트랙트에 Chaincode라는 호칭을 사용하고 있다. Chaincode는 현재 프로그래밍 언어 중에서 Go나 Java로 작성할 수 있으며 상태 저장 데이터베이스로는 CouchDB[14]를 사용한다.

12) http://www.riss.kr/link?id=T14372753
13) 프로그램 분산버전관리 도구인 깃(Git)을 지원하는 대표적인 웹 서비스

그림 4 Fabric의 트랜잭션 처리흐름[15)]



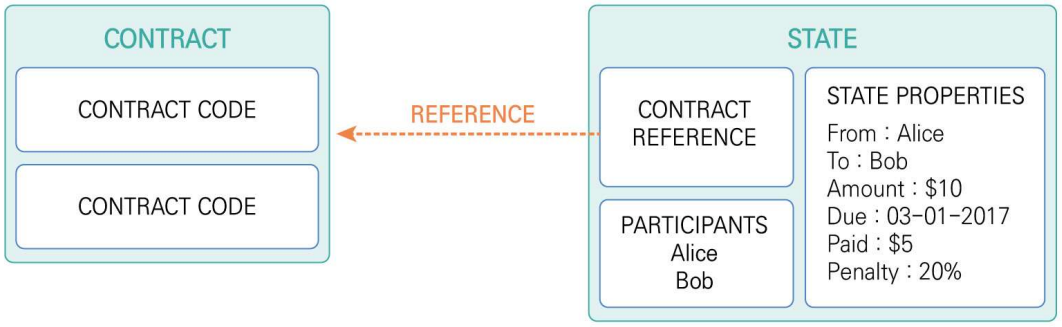
Fabric은 [그림 4]와 같이 트랜잭션 및 Chaincode의 검증과 블록생성 기능을 분리하여 검증은 Endorser 노드(endorsing peer)가 수행하고 블록 생성 및 공유는 Orderer 노드(orderer)가 수행한다. 세부적으로, 먼저 클라이언트는 트랜잭션을 생성하고 검증을 위해 Endorser들에게 전송([그림 4]의 ①)한다. 그 다음 Endorser는 트랜잭션을 검증[16)] 및 실행하고 검증결과와 상태[17)]에 서명하여 클라이언트에게 반환([그림 4]의 ②)한다. 클라이언트는 정상 반환 메시지(transaction-endorsed)가 각 Chaincode에서 요구되는 개수만큼 반환되면 트랜잭션과 상태를 Orderer에게 전송([그림 4]의 ③)하여 블록에 포함되도록 한다. 마지막으로 Orderer는 수집된 트랜잭션과 상태를 연대순 정렬하여 블록을 생성하고 모든 노드(endorsing 및 committing peer)에 전파하고 노드는 트랜잭션의 서명값을 검증하여 문제가 없을 경우 데이터베이스에 반영([그림 4]의 ④)한다.

14) 분산서버클러스터 환경에 적합한 형태로 개발된 Apache 재단의 공개 데이터베이스
15) https://hyperledger-fabric.readthedocs.io/en/latest/arch-deep-dive.html
16) 트랜잭션의 포맷, 트랜잭션의 재사용 여부, 클라이언트의 서명, 트랜잭션 및 Chaincode의 정상실행 여부 등 확인
17) 트랜잭션에 따라 실행된 Chaincode의 결과 값(계좌 잔고, 기타 변수 및 데이터)

또한 Fabric은 기밀성 보장이 필요한 거래를 위해 블록체인 네트워크 내에서 소규모 네트워크를 구성할 수 있도록 채널(Channel)이라는 기능을 지원하며 [그림 4]는 채널별로 진행된다. IBM은 이러한 요소를 바탕으로 스마트 컨트랙트를 이용한 물류 프로세스 간소화 프로젝트를 진행하고 있다.

R3는 대형 글로벌 은행 주도로 80여 개의 은행이 참여하여 공동으로 구성한 블록체인 컨소시엄이다. R3는 2016년 12월 자신의 블록체인 플랫폼인 Corda를 공개했는데 Corda는 금융권 요구사항을 만족하기 위하여 네트워크에 참여하는 모든 노드들이 데이터를 공유하는 기존의 블록체인 구조를 벗어나 이해 당사자들만 데이터를 공유하는 블록체인 플랫폼이다.

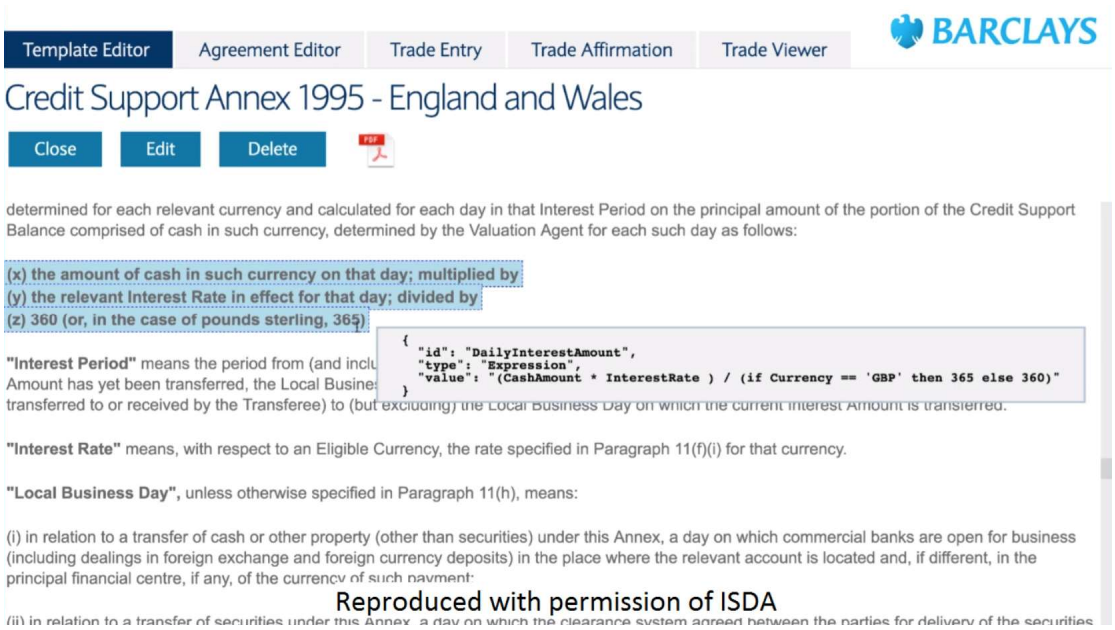
그림 5 R3 Corda 동작 방식[18)]



Corda의 스마트 컨트랙트는 실제 코드로 구성된 계약 코드(Contract Code)와 계약의 상태인 볼트(Vault), 그리고 실제 제도권에서 사용하는 법적인 문서들을 지원하기 위한 법률언어(Legal Prose)로 구성된다. 각 볼트는 계약 코드와 법률언어에 대한 링크를 가지고 있다. 한 계약에 대한 볼트는 전부 연결되어 있으며 이는 다른 스마트 컨트랙트와 유사하다. 또한 각 볼트에 법률언어를 링크하여 각 볼트가 어떤 법률 베이스로 작성되었는지 보장된다.

18) https://brunch.co.kr/@jeffpaik/29

그림 6 Corda의 Smart Contract Template[19)]



R3는 더욱 사용자 및 법률 친화적인 스마트 컨트랙트 기능을 제공하기 위하여 영국의 Barclays 은행과 함께 실제 계약서로 변형 및 계약서 상태에서 계약내용을 변경할 수 있는 스마트 컨트랙트 템플릿 개발 프로젝트를 수행하였다. 이 프로젝트의 목표는 개발자가 아닌 법률 전문가가 쉽게 스마트 컨트랙트 기반의 계약을 작성하고 수정할 수 있도록 하는 것이며, 이러한 스마트 컨트랙트 템플릿은 리카르디안 컨트랙트[20)](Ricardian Contract)의 일종으로서 실제 계약서로 출력할 수 있다는 장점이 있다. Corda의 스마트 컨트랙트 템플릿 예시는 [그림 6]과 같다.

Corda는 블록체인 외부의 정보에 의해 각 노드 별로 스마트 컨트랙트의 실행 결과가 상이해질 수 있는 문제를 해결하기 위해 Oracle이라는 기능을 제공한다. 예를 들어, 어떤 스마트 컨트랙트에 특정시간의 주가, 금리, 날씨,

19) https://vimeo.com/168844103
20) 일반 사람들이 이해 가능한 법률적 언어와 컴퓨터 S/W가 이해 가능한 프로그래밍 언어(계약 코드) 및 데이터로 구성된 계약서로서 일반적으로 법률적 계약 조건에 관련된 계약 코드 및 데이터가 링크되어 있는 형태

환율 등의 정보가 사용될 경우 노드가 위치한 국가 및 지역, 정보 제공기관 등에 따라 스마트 컨트랙트의 실행 결과가 달라질 수 있다. 이 경우 계약 당사자 간의 분쟁이 발생가능하며 블록체인의 신뢰성이 저하될 수 있다. 이를 방지하기 위해 Corda는 네트워크에 포함된 노드가 외부 정보를 조회할 수 있는 단일화된 창구로써 Oracle을 제공한다.

3. loopchain SCORE(Smart Contract on Reliable Environments)

loopchain[21]은 theloop에서 개발하는 블록체인 플랫폼으로 [그림 7]과 같이 모듈화된 아키텍처를 기반으로 BFT[22] 계열의 합의알고리즘과 스마트 컨트랙트를 지원하는 블록체인 플랫폼이다. theloop는 loopchain의 스마트 컨트랙트인 SCORE를 이용하여 인증 서비스, 보험 청구 서비스, 채권 거래 서비스를 개발 및 서비스할 예정에 있다.

loopchain의 SCORE는 Chaincode와 마찬가지로 합의 엔진과 SCORE 처리 로직이 분리되어 인터페이스만 동일하면 어떠한 개발환경에서 SCORE를 개발하여도 구현이 가능하며 현재는 Python만 지원하고 있다. 또한 기존의 Key-value 데이터베이스뿐만 아니라 업무의 효율성을 위해 관계형 데이터베이스 등 다양한 데이터베이스를 사용할 수 있다는 특징이 있다.

SCORE는 기존 스마트 컨트랙트가 변경될 경우 일시적으로 해당 스마트 컨트랙트의 서비스가 중단될 수 있어 이를 버전 별로 관리할 수 있도록 하여 무중단 환경에서 스마트 컨트랙트 업데이트를 지원한다. 또한 R3 Corda의 Oracle과 유사한 기능을 제공하는 loopchain의 Portal[23] 기능을 통해 기존 스마트 컨트랙트에서 외부 서비스의 응답을 받지 못하는 문제를 해결하였다.

---

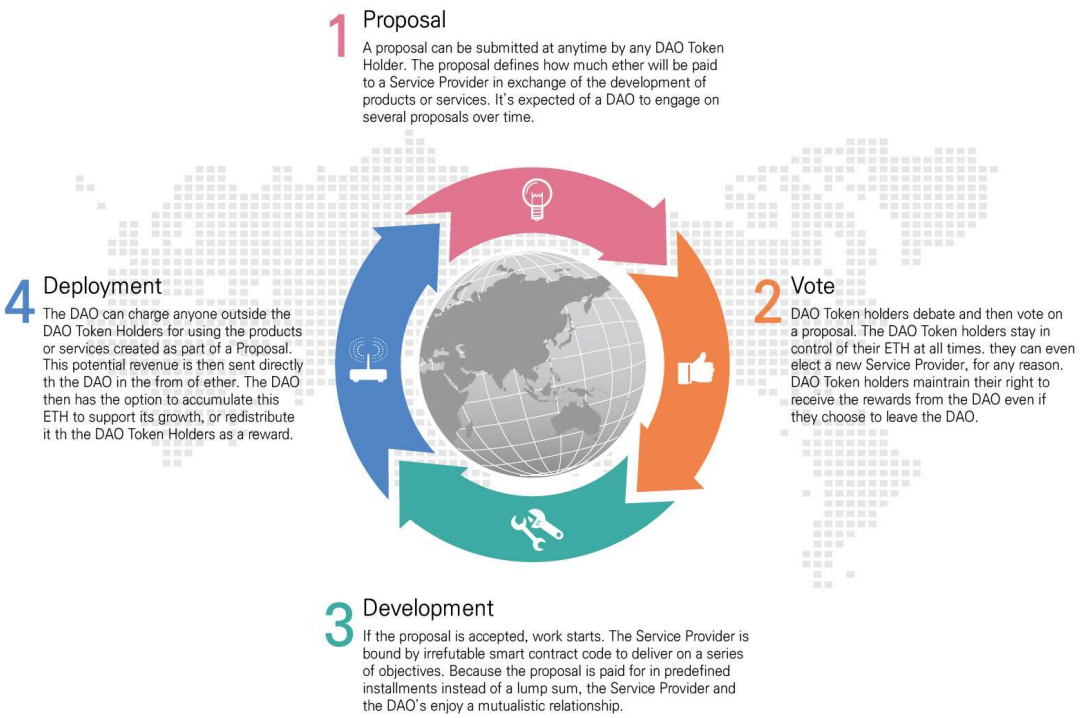
21) https://blog.theloop.co.kr
22) BFT(Byzantine Fault Tolerance) 알고리즘은 분산 컴퓨팅 환경에서 사용되는 합의 알고리즘으로 전체 노드 중 일부가 악의적인 노드인 경우에도 정상적인 합의가 가능하도록 고안된 방식
23) 외부 서비스 호출 신뢰 보장 과정

Ⅳ 스마트 컨트랙트 적용 사례

1. DAO, Crowd Token Sale

DAO와 Crowd Token Sale은 공개 블록체인 기반 스마트 컨트랙트 플랫폼인 이더리움에서 가장 활발하게 사용되었던, 또는 사용되고 있는 스마트 컨트랙트이다. 이러한 스마트 컨트랙트들은 자체 토큰을 이더리움을 통해서 판매하는 서비스이다. 토큰은 생성 목적에 따라 새로운 서비스를 이용할 수 있는 권한, 특정 조직의 의사결정을 할 수 있는 권한, 나중에 새로운 가상화폐를 얻을 수 있는 권한 등을 나타낼 수 있다.

그림 7 DAO 의사 결정 프로세스[24)]



24) themerkle.com

앞서 언급 하였듯이 일련의 해킹 사태로 지금은 사라진 DAO는 이더리움 업계에 가장 큰 영향을 끼친 토큰 중 하나이다. DAO는 자율화된 분산 조직 개념으로 DAO토큰을 구매한 유저는 주주로서 DAO가 나아갈 방향성에 대해 의사 결정을 수행할 수 있었다. DAO는 많은 사람들에게 관심을 받았으며 이더리움 가격에도 큰 영향을 미쳤다.

그러나 이상적인 분권화된 조직 개념에도 불구하고 실제 DAO의 주주권을 이용한 투표를 통해 단 한 건의 의제도 통과하지 못하였다. 또한 이후에 스마트 컨트랙트 소스코드의 취약점을 이용하여 해커들이 DAO 컨트랙트에 공격을 시도했으며 하드 포크로 모든 DAO토큰이 환불 처리되면서 DAO는 사라졌다.

DAO 이후에도 많은 토큰이 이더리움을 통해 발행되었는데 그중 가장 큰 이슈가 되었던 것은 Crowd Token Sale이다. 흔히 ICO라 불리는 Crowd Token Sale은 새로운 DAPP(Decentralized Application)이나 새로운 가상화폐를 만들기 전에 개발 비용을 이더리움을 통해 모금하고 새로 개발되는 상품에 대한 권리(토큰)를 주는 것이다. 대부분의 ICO 토큰은 프리세일 가격보다 개발이 완료되어 실제 거래될 때 가격이 증가하였기 때문에 새로운 ICO를 시작하면 많은 투자자가 투자를 하게 되었고 이때 이더리움 네트워크에 트래픽이 몰려 네트워크가 늦어지는 현상까지 발생하였다.

스마트 컨트랙트 기반의 ICO 토큰 발행이 주목 받음에 따라 보안의 중요성도 강조되고 있다. 예로 DAO 해킹사건 이후로 유사한 사고를 방지하기 위해 표준 컨트랙트 양식과 스마트 컨트랙트 코드의 보안성을 검증하는 업체가 생겨났으며, 실제 ICO 토큰 발행을 위한 스마트 컨트랙트에 활용되고 있다.

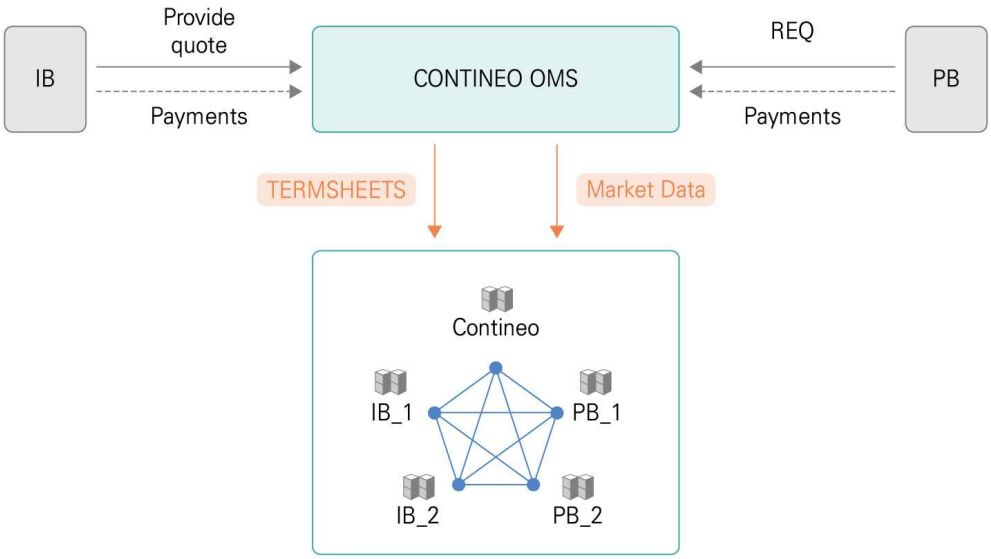
2. 채권 및 파생상품 거래

Contineo[25]는 글로벌 기업 간 다양한 금융 상품을 디지털로 거래할 수 있게 하는 플랫폼 스타트업이다. Contineo는 금융상품의 제공자와 수요자를

25) http://contineo.link/

네트워크로 연결 시켜주고 네트워크를 통해 계약을 수행하는 플랫폼을 개발하였다. Contineo는 해당 네트워크의 신뢰도를 향상시키기 위하여 금융상품 계약 체결 후 이행하는 인프라를 블록체인 스마트 컨트랙트를 통해 수행하는 프로젝트를 진행 중이다.

그림 8 Contineo 인프라 구조

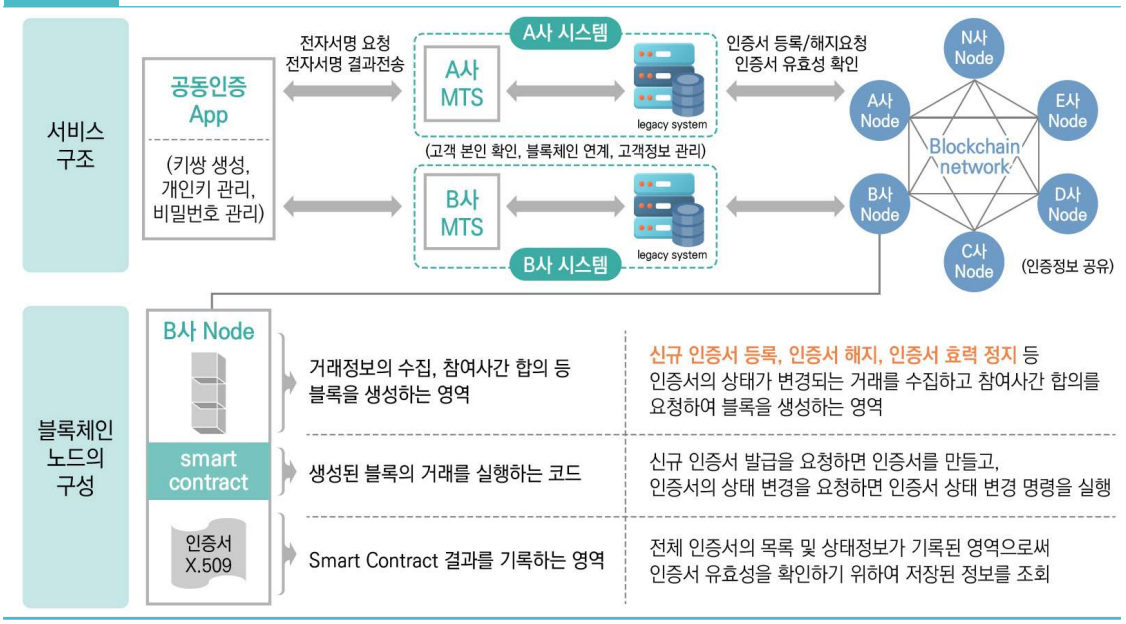


[그림 8]은 Contineo 블록체인 이용에 관한 설명도이다. Contineo를 통해 두 회사가 계약을 맺으면 각 이해관계자의 서명을 포함하여 계약 정보와 체결 데이터를 블록체인에 올린다. 스마트 컨트랙트는 스마트 컨트랙트 계약의 내용에 따라 자동으로 이행한다. 예를 들어 KOSPI 가격에 따라 청산 가격이 달라지는 계약을 맺으면 스마트 컨트랙트는 KOSPI 가격에 따라 자동으로 청산 가격을 조정하며 만기일이 되면 청산해준다. Contineo는 이러한 스마트 컨트랙트 기능을 통해 주식연계채권, 장외주식 등의 금융상품 거래 시스템의 구축을 지원한다.

3. 금융투자업권 공동 인증

금융투자업권 공동 인증 서비스는 loopchain과 loopchain의 스마트 컨트랙트인 SCORE를 이용하여 인증서를 발급 관리하는 서비스이다. 금융투자업권 공동 인증 서비스는 새로운 인증서의 발급 또는 상대 회사의 인증서 검증을 위해 블록체인에서 인증서를 발급하고 유효성 검증을 수행할 수 있는 기술이다. 세부적으로, 스마트 컨트랙트에 인증서의 상태 정보가 등록·관리되어 해당 블록체인을 이용하는 기관은 다른 회사에서 발급한 인증서를 스마트 컨트랙트를 통해 간단히 검증할 수 있다.

그림 9 금융투자업권 공동 인증 서비스 구조



금융투자업권 공동 인증 서비스의 가장 큰 특징은 인증서 발급 관리 역할을 블록체인 상의 SCORE에서 수행하는 것이다. [그림 9]에서 보듯이 각 사의 시스템은 자신의 블록체인 노드에 인증서 발급 검증을 요청하며 블록체인은 요청에 따라 인증서를 발급하고 유효성을 검증한다. 이때 인증서 발급 관리 SCORE를 사용하며 블록생성 시 해당 블록에만 유효한 서명키를 생성하여 인증서에 서명함으로써 인증서 발급 기관의 역할을 수행할 수 있다.

V 결 론

스마트 컨트랙트 기술에 대한 개념이 90년대 처음 소개 된 이후, 디지털 상에서 신뢰 네트워크를 구축할 수 있는 기술인 블록체인이 발명되어 스마트 컨트랙트가 최초로 세상에 구현되었다. 블록체인의 스마트 컨트랙트를 이용하여 사용자들은 신뢰를 보장하기 위해 사용하였던 다양한 계약을 스마트 컨트랙트 코드로 대체할 수 있게 되었다. 아직은 시작 단계인 기술이지만 기관의 주주권 구매와 권리 행사, 사설 인증서 배포, 다양한 토큰들을 블록체인을 통해 배포하는 등 스마트 컨트랙트를 이용한 다양한 시도들이 있었다.

스마트 컨트랙트 기술은 블록체인의 유형 및 플랫폼에 따라 특성이 달라진다. 대표적인 공개 블록체인인 이더리움의 스마트 컨트랙트는 공개된 네트워크에서 그 신뢰도를 보장하기 위하여 모든 참여자들이 스마트 컨트랙트에 대한 요청을 실행하고 스마트 컨트랙트의 상태를 저장한다. 이러한 공개 블록체인의 스마트 컨트랙트는 자체 가상화폐를 이용한 스마트 컨트랙트를 만들 수는 있으나 블록체인 외부의 데이터에 대한 접근이 제한되고 모든 데이터가 공유되어 기밀성을 보장하기 어려운 문제가 있어 토큰 발행, 주식 발행 등의 서비스에 한정적으로 활용되고 있다. 그 외 사설형 블록체인인 Hyperledger Fabric, R3 Corda, loopchain의 경우 각 블록체인 모델에 따라 데이터 공유 주체가 다르고, 외부 데이터에 대한 접근이 제한적으로 허용된다.

기관 간의 신뢰를 구축하기 위해 발생하는 시간적, 비용적 문제는 사설형 블록체인 기반 스마트 컨트랙트를 통해 해결할 수 있다. 스마트 컨트랙트를 기반으로 하는 사설 인증서 발급, 기관 간 계약 이행, 물류 계약 단순화 등의 업무의 증명 테스트가 수행되거나 실제 서비스가 준비되고 있다. 이러한 스마트 컨트랙트를 이용하면 기존의 신뢰 문제로 인해 확장이 어려웠던 업무를 쉽게 처리하고 다양한 업무에 신뢰를 제공하여 금융, 공공, 물류, 교육 등 전 영역에 걸쳐 혁신적인 서비스들이 출현할 것으로 예상된다.

참고문헌

[1] Bitcoin : A Peer-to-Peer Electronic Cash System, Satoshi Nakamoto, 2008.11.

[2] SZABO, Nick. The idea of smart contracts. Nick Szabo's Papers and Concise Tutorials, 1997.

[3] Buterin, Vitalik. "Ethereum Whitepaper". github. Retrieved 1 June 2017.

[4] Cachin, Christian. "Architecture of the Hyperledger Blockchain Fabric" (PDF). ibm.com.

[5] 고동휘, 블록체인 기반 스마트 계약에서 외부 인터페이스를 위한 분산합의 연구, A study on distributed consensus for external interface in blockchain based smart contract, 석사학위논문, 2017.

[6] Atzei, Nicola; Bartoletti, Massimo; Cimoli, Tiziana , "A survey of attacks on Ethereum smart contracts" (PDF), 6th International Conference on Principles of Security and Trust (POST), European Joint Conferences on Theory and Practice of Software, 2017

[7] 블록체인 활용 사례로 알아보는 금융권 적용 고려사항, 금융보안원, 2016.01.

[8] 금융권 블록체인 활용 방안에 대한 정책 연구, 금융보안원, 2016.04

[9] I. Grigg. The Ricardian Contract. In Proceedings of the First IEEE International Workshop on Electronic Contracting, pages 25-31. IEEE, 2004

[10] Clack, Bakshi, Braine, "Smart Contract Templates: foundations, design landscape and research directions," 2016

[11] David Siegel , Understanding The DAO Attack, Coindesk, 2016. 06

[12] Mike Hearn, Corda: A distributed ledger, R3CEV Tech. paper, 2016. 12