오픈소스 블록체인 기술 동향

최윤철 한국전자통신연구원 지능정보표준연구실 선임연구원
박정수 한국전자통신연구원 지능정보표준연구실 책임연구원

1. 머리말

블록체인은 네트워크 내의 모든 참여자가 공동으로 거래 정보를 검증하고 기록함으로써 공인된 검증 기관이 없이도 거래 기록의 무결성 및 신뢰성을 확보한다. 또한 블록체인은 해시(hash), 전자서명(digital signature), 암호화(encryption) 같은 보안 기술(cryptography)을 활용해 거래 정보를 기록한 분산 장부를 네트워크에 속한 모두와 공유한다.

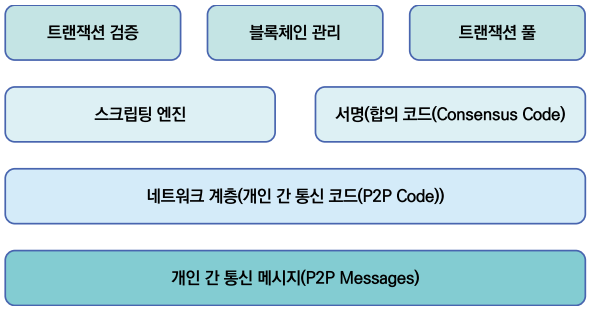
이 블록체인 기술은 여러 가지 환경에 따라 다양하게 구현될 수 있다. 이 구현물들을 블록체인 플랫폼이라고 하며 이 플랫폼을 탑재한 노드들로 분산형 블록체인 네트워크를 구축한다. 이 분산형 네트워크 인프라상에서 다양한 블록체인 응용이 개발 중이며 현재 블록체인 플랫폼들과 함께 오픈소스로 제공된다.

본고에서는 ISO/TC 307(블록체인 및 분산원장기술 기술위원회)의 용어 표준에서 제시된 방식에 따라 오픈소스 블록체인 플랫폼들을 분류해 소개한다. ISO/TC307은 블록체인 레코더에 대한 접근 허가 여부에 따라 비허가형과 허가형으로 분류한다. 그래서 본고에서는 대표적인 비허가형과 허가형 블록체인 플랫폼과 오픈소스 현황을 소개한다.

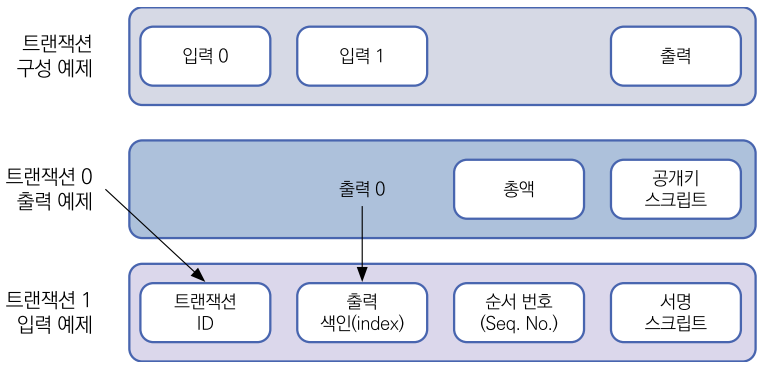
2. 비허가형 오픈소스 블록체인 플랫폼

2.1 비트코인 플랫폼

비트코인은 사토시 나카모토라는 신원 미상의 인물이 발표한 논문에서 시작해 개인 간 통신(P2P) 네트워크상에 구현한 가상 화폐 프로젝트로 데이터를 모든 노드와 공유한다. 이 데이터는 블록 단위의 체인 형태로 저장되며 각 블록마다 이전 블록의 해시 정보를 포함해 비가역적 특성을 가진다. 비트코인 합의 알고리즘은 해시 함수 기반 작업증명 방식을 사용한다. 비트코인에서는 공개키와 개인키를 사용한 사용자 인증 및 검증을 수행한다.



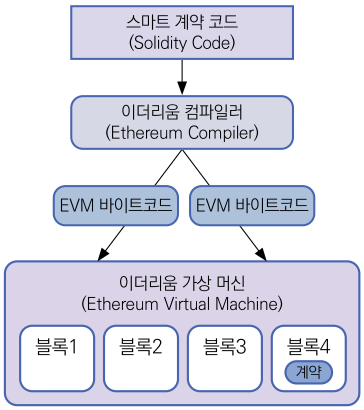
[그림 1] 비트코인 플랫폼



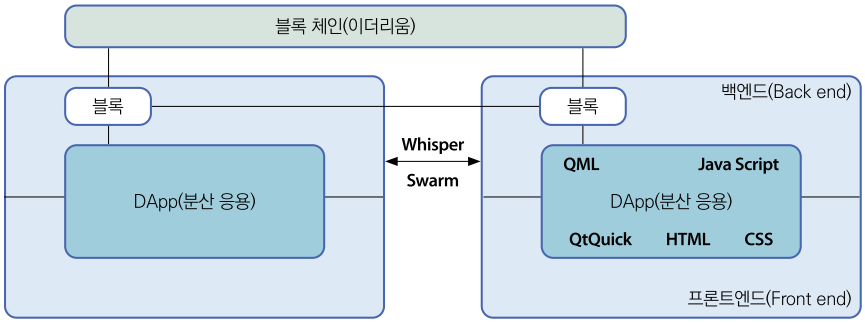
[그림 2] 비트코인 트랜잭션 구조

비트코인 플랫폼 구조는 [그림 1]과 같이 개인 간 통신 지원 메시지 모듈, 네트워크 계층 모듈, 스크립팅 엔진 모듈, 서명 모듈, 트랜잭션 검증 모듈, 블록체인 관리 모듈, 트랜잭션 풀 모듈로 구성된다. 비트코인 플랫폼에서 주고받는 트랜잭션은 [그림 2]와 같이 4바이트 트랜잭션 버전 번호로 구분되며 일반적으로 하나의 출력과 하나 이상의 입력으로 구성된다. 각 트랜잭션의 입력은 이전 출력의 지불 금액을 사용한다. 출력(example output)은 출력 색인 번호, 지불 금액(amount) 및 공개키 스크립트(pubkey script)로 구성된다. 제시된 공개키 스크립트의 조건이 만족되면 지불 금액(amount)만큼 지출 가능하다. 그리고 예시 입력(example Input)은 트랜잭션 식별자(transaction identifier), 출력 인덱스, 순서 번호 및 서명 스크립트로 구성된다. 트랜잭션 식별자는 이전 트랜잭션에서 순서대로 획득하며 출력 인덱스는 사용되는 특정 출력을 식별하고자 예시 출력을 활용해 결정한다. 서명 스크립트는 공개키 스크립트의 조건을 만족하는 데이터 제공자의 서명 값이다.

블록체인 프로토콜이 어느 한 시점에서 급격하게 변경되는 하드포크를 통해 비트코인에서 비트코인 골드, 비트코인 다이아몬드 같은 프로젝트들이 생성됐다. 그리고 비트코인을 활용하면서 발생하는 문제들을 해결하면서 파생된 프로젝트도 있는데, 처리속도 문제 및 거래 수수료 문제로 파생된 라이트코인 프로젝트가 그 예이다. 비트코인에서 저장 문제로 서명을 분리하는 업그레이드를 진행했을 때 블록사이즈를 8MB로 변경해 파생된 비트코인 캐시도 있다.



[그림 3] 이더리움 스마트 계약 실행 구조

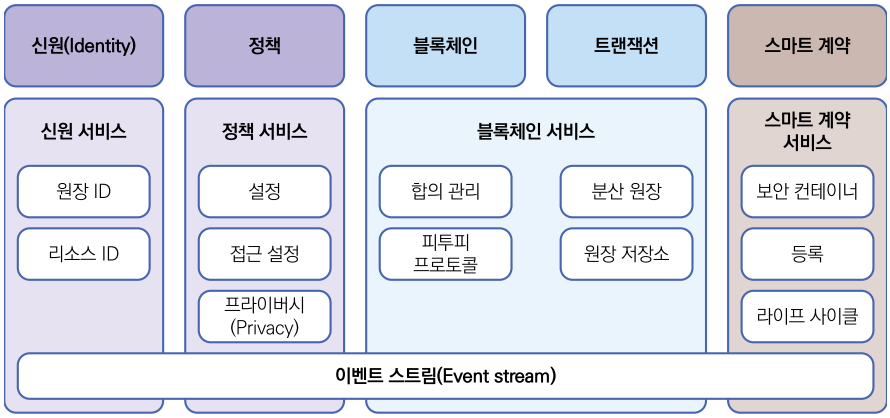


[그림 4] 이더리움 분산 응용 구조

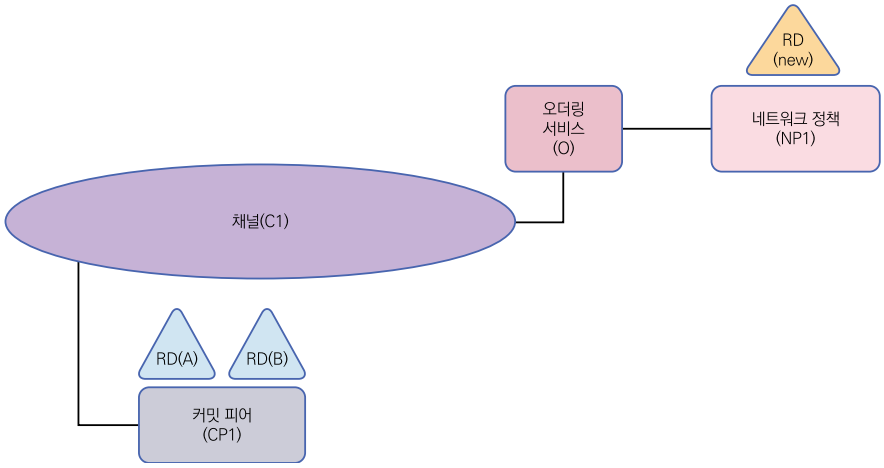
2.2 이더리움(Ethereum) 플랫폼

이더리움은 금융 이외의 다양한 분야에서 블록체인을 적용하고자 시작됐다. 이더리움의 특징은 튜링 완전성을 갖춘 확장형 언어로 스마트 계약을 지원하며 이를 기반으로 다양한 응용 구현이 가능하다는 점이다. 이더리움은 작성된 스마트 계약을 컴파일해 바이트 코드 형태로 디코딩한다. 이 디코딩 데이터는 합의 알고리즘에 따라 이더리움 네트워크에 저장되고 실행된다. 여기서 이더리움 네트워크는 개인 간 통신 네트워크상에서 다른 이더리움 노드와 연결된다. 이더리움 네트워크는 개인 간 통신 네트워크상에서 효율적인 서비스를 제공하고자 다양한 프로토콜을 사용한다. IPFS(InterPlanetary File System)는 이미지, 비디오 파일 같은 대용량 파일을 저장하는 데 사용하고, 스웜(Swarm) 프로토콜은 데이터 동기화 및 검색에 사용한다. 그리고 위스퍼(Whisper) 프로토콜은 개인 간 통신 메시지를 전송할 때 사용한다.

이더리움의 주요 특징인 스마트 계약은 일종의 컴퓨터 프로그램이다. [그림 3]과 같이 스마트 계약 코드로 작성되고 바이트 코드로 변환돼 이더리움 가상 환경(EVM, Ethereum Virtual Machine)상의 블록에 저장된다. 다시 말해, 스마트 계약은 EVM용 프로그래밍 언어로 기술된 소스 코드이다. 이 프로그래밍 언어에는 Solidity, Vyper, LLL, Bamboo, Serpent 등이 있다. 다만 스마트 계약 소스 코드를 이더리움 플랫폼상에서 실행하려면 EVM에서 실행되는 저수준 바이트 코드로 컴파일돼야 한다. 컴파일



[그림 5] 하이퍼레저 패브릭 구조



[그림 6] 하이퍼레저 패브릭 네트워크

후에 계약 생성 트랜잭션을 사용해 이더리움 플랫폼에 배포된다.

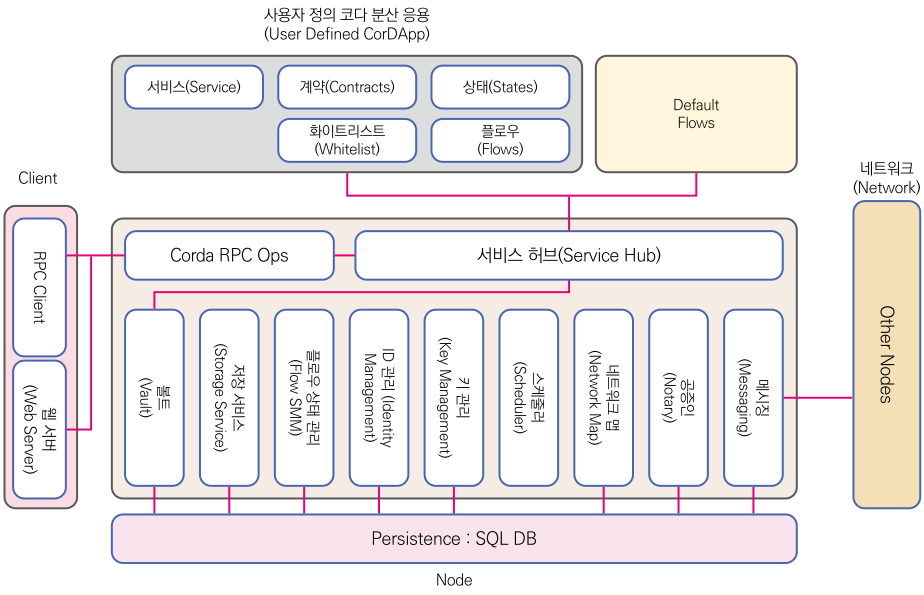
이더리움 플랫폼은 분산 응용을 위해 [그림 4]와 같은 백엔드 및 프론트엔드 개발 언어를 사용한다. 또한 이러한 분산 응용 간에 메시지 및 데이터를 주고받고자 위스퍼와 스웜 프로토콜을 사용한다. 위스퍼 프로토콜은 가십(Gossip) 프로토콜 기반의 메시지를 전송하는데, 위스퍼 프로토콜을 사용하면 메시지에 대한 보안 레벨을 설정할 수 있다. 그리고 스웜 프로토콜은 분산 스토리지 환경에서 저장된 데이터를 동기화하고자 개발한 프로토콜이다.

현재 이더리움 플랫폼에 있는 보안 및 확장성 문제를 해결하기 위해 이더리움 2.0 프로젝트가 진행 중이다. 그리고 통신사 네트워크에서 사용하는 로밍 비용 정산 및 망 사용료 부과나 자산 관리 프로젝트에도 이더리움을 활용한다. 특히 이더리움은 스마트 계약 및 분산 응용을 구성할 수 있다.

3. 허가형 오픈소스 블록체인 플랫폼

3.1 하이퍼레저 패브릭 플랫폼

하이퍼레저는 IBM 주도로 개발된 모듈식 구조의 블록체인 플랫폼이다. 이 모듈식 구조는 모듈 수정 및 재구성을 통해 다양한 플랫폼으



[그림 7] 코다 플랫폼 구조

로 확장할 수 있으며 시험용 라이브러리 모듈도 개발할 수 있다. 대표적인 하이퍼레저 플랫폼이 [그림 5]와 같은 패브릭 구조이다.

본고에서는 하이퍼레저 패브릭 2.2 버전을 중심으로 오픈소스 주요 기능을 소개하겠다. 패브릭 구조는 전용 블록체인(private blockchain)으로 개발됐지만 개방형 블록체인(public blockchain)으로도 사용 가능하다. 그리고 다양한 블록체인 플랫폼을 지원할 수 있도록 기능 모듈 단위로 개발돼 기능 추가와 변경이 쉽다.

하이퍼레저에서는 기존 블록체인 플랫폼에서 정의한 스마트 계약을 '체인 코드'라고 부른다. 이것은 이더리움 체인코드에서 상태값에 변화를 주고, 원장에 업데이트를 하는 로직에 해당한다. 그리고 권한에 따라 한 네트워크에 있더라도 접근할 수 있는 체인 코드가 다르다. 합의 알고리즘은 특정 조건에 의해 승인된 업데이트만을 선택해서 체인 코드를 실행한다. 또한 여러 트랜잭션이 동시에 발생하면 순서에 맞게 배열을 수행하고 오류가 없는 경우에만 실제 원장에 반영된다.

이러한 하이퍼레저 패브릭 네트워크는 [그림 6]과 같이 오더링 서비스(O), 네트워크 정책(NP), 클라이언트 애플리케이션(CA), 애플리케이션을 소유한 네트워크 참가 조직(RD)으로 구성된다. 비트코인 또는 이더리움에서 사용하는 합의 알고리즘을 대신해 하이퍼레저 패브릭에서는 오더링 서비스를 사용한다. 오더링 서비스에서는 네트워크 내의 채널(오더링 서비스 채널은 네트워크 내 컴포넌트 간의 전용 통신을 의미한다. 채널 설정값에 따라 추가 인증 과정 후에 가입이 가능하다)에 대한 구성 정보를 소유하며 이를 기반으로 관리자 역할을 한다. 그리고 오더링 서비스에서는 채널 정보가 포함된 블록을 생성한다.

하이퍼레저에는 블록체인 플랫폼을 구성하는 패브릭 이외에도 다양한 블록체인 구성 플랫폼이 있다. 또한 이러한 블록체인 플랫폼과 연동이 가능한 관련 라이브러리 및 도구 프로젝트도 개

발되고 있다. 이외에도 패브릭을 활용해 월마트에 공급되는 망고의 이력을 추적하거나 공급사슬 관련 유즈케이스 및 기업 간 전자 거래 환경을 구축한 사례가 있다.

3.2 코다 플랫폼

코다는 금융서비스에 특화된 블록체인 플랫폼 개발을 목적으로 'R3'라는 블록체인 컨소시엄에서 개발했다. 금융서비스 특화를 목표로 했기 때문에 금융기관, 거래소 및 관련 업체들이 주로 참여해 컨소시엄을 구성한 것이다. 코다는 금융서비스 특성상 블록체인에 참여하는 노드들이 서로 주고받는 메시지 보안을 강조한다. 코다는 거래 데이터를 비공개로 할 수 있다. 또한 자바 또는 자바 가상 머신(JVM, Java Virtual Machine) 기반의 다양한 언어로 스마트 계약을 할 수 있다. 또한 기존 블록체인 플랫폼과는 달리 거래 유효성과 계약 검증 과정을 분리한다. 거래 유효성은 거래에 참여하는 노드 간에 서명을 기반으로 합의하고 계약 검증은 검증 노드를 통해 수행된다. 이러한 합의 알고리즘의 특성 때문에 다른 블록체인 플랫폼에 비해서 초당 거래 처리 속도(TPS)가 높다.

코다 플랫폼은 은행과 같은 금융회사가 참여하는 컨소시엄에서 출발했기 때문에 이를 기반으로 한 프로젝트는 금융회사 간 거래 자동화에 활용된 유즈케이스가 대부분이었다. 그러나 최근에는 코다에서 지원하는 분산 응용을 활용하는 다양한 오픈소스 프로젝트도 진행 중이다.

4. 맺음말

본고에서는 오픈소스 블록체인 기술을 사전 인증 서비스 유무에 따라 허가형과 비허가형으로 구분했다. 그리고 블록체인 플랫폼을 탑재한 노드들이 블록체인 네트워크에 참여하기 위해 인증 과정을 거치는 허가형 오픈소스 기반 블록체인 플랫폼인 비트코인과 이더리움 구조에 대해서 살펴보았다. 또한 인증 절차 없이 바로 블록체인 네트워크에 참여할 수 있는 비허가형 오픈소스 기반 블록체인 플랫폼인 하이퍼레저 및 코다 구조에 대해서 살펴봤다.

참고문헌

[1] TTA, TTAR-10.0138, 오픈소스 블록체인 기술 동향(기술보고서), 2020.10

[2] Bitcoin Developer Guides, https://developer.bitcoin.org/devguide/index.html

[3] Ethereum Developer Resources, https://ethereum.org/en/developers/#getting-started

[4] Hyperledger Fabric Doc, https://hyperledger-fabric.readthedocs.io

[5] Corda Key Concepts, https://training.corda.net/key-concepts/concepts