이더리움이란

네이버 시사상식사전에는 “블록체인 기술을 기반으로 한 가상화폐의 일종”이라고 나옵니다. 이 설명만으로는 단순히 차기 비트코인 정도로밖에 보이지않는데요, 정작 이더리움은 2015년 당시 블록체인 2.0, 차세대 블록체인이라 불리며 데뷔했습니다.

왜 차세대 비트코인이 아니라 차세대 블록체인일까요.

이더리움은 기존의 비트코인처럼 전통적인 화폐를 대체하기위한 새로운 지불수단으로서의 가상화폐가 아닙니다. 또한 비트코인 출시 이후, 비트코인이 가지고있던 한계들을 보완하기 위해 출시된 수 많은 자기보완적 알트코인들 수준에 그쳐지는 것도 아닙니다.

물론 비트코인과 비교하면 처리용량, 속도, 옵션 추가등의 면에서 더 발전된 형태의 수단이기도 합니다만, 이더리움의 진정한 가치는 단순한 지불 수단이 아닌 다양한 Smart Contract와 이를 바탕으로 한 Decentralized App을 구현할 수 있는 플랫폼이라는 점에 있습니다.

이번 발표에서는 이러한 Ethereum을 표현하는 세가지 키워드 BlockChain, Smart Contract와 dApp 마지막으로 부가적인 사항들을 다루겠습니다.

Block Chain

그동안 공부했던 BitCoin의 BlockChain과 대체적으로 동일합니다. 노드들은 지속적으로 상호간   
통신을 통해 발생한 Transaction들을 추가해가며 일련의 검증과정을 거쳐 Block을 생성해냅니다. 거기에 추가로, 기존 BitCoin BlockChain이 가지고 있던 문제점들을 지속적으로 보완하는 모습을 보여주는데, 예시로 DAG 구조를 이용한 채굴파워 집중방지, Stale Block(BitCoin에서 Orphan블럭)처리를 위한 GHOST Protocol, 최근 결정된 사항인 PoW에서 PoS로의 합의알고리즘 변경, 기존 PoS의 한계를 보완한 Slasher Protocol 및 Casper Protocol의 추가 등이 있습니다.

또한 Ethereum BlockChain에서 각 노드들은 최초의 블록을 포함한 전체 블록체인의 정보를 가지고 있고, 지갑의 역할로써 계좌생성요청, 이체, 잔고확인등의 UI적 기능을 할 수 있으며, 각자 블록 마이닝이 기여하기도 하고, Smart Contract의 내용을 담거나, dApp으로써의 기능을 하기 위해 필요한 Ethereum Virtual Machine을 포함하고 있습니다. 노드들 중에는 Geth Node라는 이더리움 재단 개발팀이 직접 관리하는 블록체인 관리용 노드도 있습니다.

Smart Contract

Smart Contract란 미리 프로그래밍 된 규칙에 따라 자동으로 실행되도록 구현한 코드조각으로써, EVM(Ethereum Virtual Machine) 코드로 작성됩니다. Ethereum의 경우 Solidity, Serpent, LLL, Mutan의 언어로 쓰여질 수 있는데 현재는 Solidty를 주로 쓰고 있습니다.

이렇게 만들어진 코드조각은 컴파일되어 16진수 Byte Code, Function Signature, Application Binary Interface 줄여서 ABI 최소한 이 세가지를 뱉어냅니다. Byte Code는 Smart Contract Code를 컴파일한 결과물이며, Function Signature는 Contract Code내의 함수 이름들을 암호화한 4바이트 값으로, 함수들이 실행될 때 transaction의 파라미터값 사용됩니다. ABI는 Contract Code가 가지고 있는 로직 코드를 실제 Application에 바인딩하기 위해 필요합니다.

덕분에, 추가 기능을 개발하기 위해서는 상당량의 코드 수정이 불가피한 비트코인과 달리 시스템확장, 개선에 매우 유연하다는 장점을 가지고 있습니다. Smart Contract 적용의 예를 들자면 계약당사자간 용역, 물류등의 대금지급등을 상세히 설정, 계약 당사자간의 동의를 통해 체인 위에 기록할 수 있고, 약속된 가치의 이더리움을 계약에 귀속시켜 이해 당사자간 동의에 의해 계약의 집행 및 해지가 가능합니다. 이를 통해 대금지급에 관한 많은 법적 분쟁이 사라질 것으로 보며, 특히 기업을 중심으로 이용이 늘어날 것으로 전망합니다.

dApp (Decentralized Applications)

탈중앙화 어플리케이션, 대표적으로 p2p 파일전송 프로그램 비트토렌트, 비트코인등이 이에 속합니다. 전통적인 중앙서버 아키텍처와 dApp의 아키텍처를 웹 어플리케이션을 통해 비교해보겠습니다. 중앙서버 웹 아키텍쳐는 웹서버라는 중앙기구에 모든 데이터들이 저장되고 개별 클라이언트들의 필요에 따라 정보를 뿌려주고 받아오는 식으로 작동합니다. 하지만 이러한 방식은 클라이언트들이 서버를 무한히 신뢰할 수 없습니다. 프라이버시 침해, 감시에 대한 우려, 해킹과 데이터 유출에 대한 위험성에 노출 되어있기 때문입니다.

분산화된 모든 노드들이 각자의 데이터베이스나 비즈니스 로직등을 서버가 아닌 로컬에 저장하고 각자 필요한 부분만 전용 브라우저를 통해 블록체인 플랫폼에서 통신합니다. web3.js 는 백엔드과 커뮤니케이션하는 기본적인 기능 또는 함수들을 묶어 놓은 라이브러리이며 임의의 계좌의 밸런스를 확인하거나, 새로운 트랜잭션을 블록체인에 올릴 때 사용됩니다. Contract ABI는 위에서 설명했듯이 contract code에 엑세스 하기위한 인터페이스입니다. web3.js는 모든 dApp들이 사용하는 기본 인터페이스를 제공, contract ABI는 각 smart contract에 필요한 함수와 변수를 사용하기위한 인터페이스를 제공한다고 생각하면 될 것 같습니다.

이더리움 재단은 이러한 특징을 가진 분산화 어플리케이션들이 모두 각 노드들에 저장됨으로써 최종상태의 이더리움 네트워크 플랫폼 위에서 대중적 사용이 이루어지기를 기대하고있습니다.

현재 지속적으로 개발중인 Ethereum dApp들입니다.

More Ethereum

마지막으로 굵직굵직한 이더리움의 역사적 사건들 및 4단계 론칭입니다. 이더리움 재단은 이더리움 프로젝트 론칭을 Frontier, Homestead, Metropolis, Serenity 이렇게 4단계로 나눴는데요, 각각 최초 블록 이후 노드들이 활성화되어 블록체인이 생성되는 단계, 대중이 아닌 개발자들을 중심으로 하여 많은 기능들이 개발되고 커뮤니티가 활성되어 이더리움 생태계를 위한 기본골격이 갖춰지는 단계, 이더리움 관련 시장이 커지면서 대중들을 위한 다양한 dApp들이 체인에 담겨 이더리움 네트워크 생태계의 진정한 면모를 갖추는 단계, 마지막으로 재단이 준비한 마지막 최종단계로, 전세계에서 발생하는 대량의 기록들을 원활하게 소화 할 수 있을 수준의 블록체인이 완성되는 단계입니다.

발표 초반부에 말씀드렸던 것처럼 이더리움은 단순한 가상화폐가 아닌 블록체인 기술 기반의 분산 네트워크 플랫폼 입니다. 그 위에서 분산형 파일저장 시스템, 분산 컴퓨팅, 분산예측시장등 컴퓨팅 산업의 효율성을 폭발적으로 높일 수 있는 잠재력이 있으며, p2p프로토콜에 전자상거래, 금융, 보험등 경제적인 차원을 입힘으로써 엄청난 혁신을 가져올 수 있을 것입니다. 또한 컴퓨팅이나 금융과 관련없는 분야들에서도 다양한 어플리케이션이 나올 것 입니다.