# 왜 블록체인을 배워야 하는가

블록체인? 우연히 이더리움을 발견하게 되었다.

시간을 거슬러 2015년 7월 올림픽이라는 정식 버전의 발표를 앞두고 있던 시점이였다.

흡사 2016년 외국계 프리미엄 햄버거가 한국에 오픈한 당일 소비자들이 길게 줄을 서서 입장을 기다리는 모습이 떠올랐다.

비록 온라인일지라도 이더리움의 열기가 대단하게 느껴졌다.

호기심이 생겨났다. 읽어 보니, 내가 알고 있고 만들어 왔던 시스템하고는 딴 판으로 다른 방식이었다.

저자는 다수 금융권의 차세대 시스템 구축 사업에 참여한 경험이 있다. 지급, 결제, 입출금 등이 비지니스 및 금융 서비스에서 핵심적인 기능이고 보안 및 정확성이 매우 중요하다라는 것을 잘 알고 있다.

이더리움은 비트코인의 블록체인 기술을 기반으로하여 스마트 계약과 분산 애플리케이션을 실행하기 위한 오픈 소스 금융 플랫폼으로 보안이 뛰어나고 신뢰할 수 있다.

벌써 시간이 흘러, 이제 블록체인은 플랫폼으로 받아들여지고 있고, 향후에도 시장은 급격하게 성장할 것으로 보인다.

블록체인을 이제는 추세적 변화로 받아들이고 배워야 할 때이다.

# 웹3을 향하는 블록체인

웹3는 블록체인 기술을 활용하여 보다 탈중앙화되고 투명한 웹을 말한다. 기존의 중앙 집중식 웹과는 다르게 분산의 블록체인을 기반으로 사용자들 간의 직접적인 통신과 거래를 한다는 차이가 있다.

현재의 웹은 중앙 집중식 구조로 인해 몇 가지 신뢰성과 보안상의 문제를 야기할 수 있다. 중앙의 서버에 장애가 발생하면 치명적이며, 해킹에 노출되어 데이터 위조 및 변경이나 개인 정보의 유출이 가능하다.

그에 반해 웹3는 블록체인을 활용하여 중앙집중식 구조의 문제점을 해결하고 더욱 신뢰할 수 있고 안전한 환경을 제공할 수 있기 때문에 웹의 미래를 대표하고 있다.

블록체인은 **분산원장**으로, 집중된 서버에 의존하지 않고 **여러 불특정 컴퓨터들이** 발생하는 거래를 암호화하여 기록한다는 것이다. 서버의 장애가 발생하기 매우 어려울 뿐 아니라 해킹으로 인한 위변조가 원천적으로 봉쇄되어 있다.

또한 **암호화폐**를 내장하고 있다는 점이 특별나다. 이런 화폐에 대해 사람들은 투자의 대상으로 여기고 큰 관심을 보이고 있다. 가격이 급등락하면서, 과연 내재가치가 있는지에 대한 논의가 뜨겁기도 하다. 지금까지 그 어떤 거래도 은행, 카드 등 금융기관에서 제공하는 플랫폼을 이용하지 않고는 가능하지 못했다. 보통 결제는 은행, 카드 그리고 요즘에는 모바일페이 등을 이용해 이루어진다. 반면에 비트코인, 이더리움과 같은 암호화폐는 이러한 신뢰할만한 기관을 거치지 않고 거래가 처리되고, 블록체인에 기록된다. 블록체인을 사용하면 이러한 **금융기관을 경유하지 않고 양자간 거래가 성립**할 수 있다는 것이다.

## 책의 특징

블록체인은 비교적 새로운 기술이기 때문에 아직 프로그래밍 강의로의 보급이 충분하지 않다.

이 책은 대학에서는 매우 빠르게 발굴하여 2016년부터 시작한 블록체인 프로그래밍 강의 내용을 묶은 것이다.

블록체인 관련 교재나 강의가 있지만 이론에 치우쳐 있는 편이고, 이 책은 블록체인 프로그래밍 실제를 배우게 된다.

이 책에서는 블록체인이 무엇인지, 어떻게 기록이 암호화, 인증, 합의, 저장되는지 배우게 된다. 필요한 이론을 배우기도 하겠지만, 프로그래밍으로 실제 해보게 된다. 블록체인 관련 가장 많이 쓰이고 있는 **이더리움**을 활용하여, 스마트계약을 만들고, 분산환경에서 블록체인으로 거래하고, 지급결제를 처리하는 것을 프로그래밍하게 된다. 최근 관심을 끌고 있는 DeFi, NFT, 웹3를 제작하는 것도 해본다.

프로그래밍 강의를 통해 블록체인 기술을 배우고 익히면 요즘 게임, 인증, 조각투자증권, NFT 등 넓어지고 있는 블록체인 산업에 진출하는 좋은 가교가 될 것이다. 블록체인 프로그래머에 대한 수요가 높아지고 있다는 점을 감안하면 많은 기회와 도전을 제공하리라 확신한다.

## 챕터별 내용

|  |  |  |
| --- | --- | --- |
| 장 | 주제 | 내용 |
| 1장 | 블록체인 소개 | 분산, 합의, 암호화페, 블록체인, 블록체인기반 화폐 |
| 2장 | 설치 geth | 스마트컨트랙, 설치, 이더리움 노드 설정 |
| 3장 | geth 네트워크 | 공중망, 사적망 |
| 4장 | 계정 | 계정, 지갑, 암호화 |
| 5장 | 거래 | 트랜잭션, 마이닝, gas |
| 6장 | 웹3 | Solidity, Remix, solc, web3.js 개발 |
| 7장 | 프로젝트 | Hello, 단순 저장, 계산 프로젝트, Solidity, solc, web3.js 개발 |
| 8장 | Solidity | 변수, 데이터 타입 |
| 9장 | Solidity | 함수 fallback, modifier |
| 10장 | Solidity | 제어구조, 데이터구조 |
| 11장 | Solidity | 컨트랙 결합, import, library |
| 12장 | DApp | DeFi 탈중앙금융 |
| 13장 | DApp | NFT 대체불가토큰 |
| 14장 | Web3 | 투표 웹디앱 |

## 필요한 것

우리는 프로그래밍을 실제 하기 때문에 **컴퓨터**가 당연히 필요하다. 윈도우, 맥 OSX, 리눅스 어느 운영체제도 무관하지만 리눅스 운영체제를 사용하는 것이 좋다. 그러나 윈도우 운영체제에서 진행해도 문제가 없다.

또한 프로그래밍 지식이 필요하다. 블록체인은 클라이언트-서버에서의 프로그래밍과는 물론 다르다. 앞서 설명한 바와같이 서버가 정해져 있지 않기 때문이다. 그러나 그 아키텍쳐에서 클라이언트와 서버가 분리되어 있는 것처럼 클라이언트는 **Javascript**, Python 등을 서버에서는 **Solidity** 언어를 사용하게 된다. 이렇게 만들어진 블록체인 프로그램을 dApp (Distributed Application)이라고 한다. dApp은 서버프로그램을 Solidity로 개발하고, 클라이언트를 Javascript 등 복수의 언어를 사용하는 것과 유사하게 여러 언어를 혼합해야 완성이 될 수 있다.

## 누가 읽어야 하나

이 책은 **암호화폐 투자와 관련한 내용이 아니다**. 또한 블록체인의 경제적, 행정적 이론을 배우는 것이 아니다. 블록체인이라는 새로운 매체에서 발생하는 금융거래를 프로그래밍으로 처리하는 내용을 다루고 있다. 기존의 온라인 결제, NFC 현장결제 등과 같은 방식과 같이 블록체인에서의 거래를 프로그램으로 만들어 보게 된다.

블록체인 프로그래밍 관련 지식과 경험을 쌓아가는 다음과 같은 상황에 이 책이 도움이 되기를 희망한다:

* 암호화폐와 같은 플랫폼에서의 거래가 어떻게 이루어지는지 배우고 싶거나,
* 실제 무엇인가 분산앱 DApp을 개발하려고 하거나,
* 특히, **물류 유통**에서와 같이 다자가 정보를 투명하게 공유해야 하거나, **개인ID**와 같이 강력한 보안이 필요하거나, **졸업증명서**와 같이 기록이 필요한 경우 등 등 창의적으로 프로젝트를 수행하고 싶은 경우

2024년 2월 25일

상명대학교 교정에서 저자가 씀