

## 01\_쉽게 이해하는 블록체인 개요

### #1

#### 1. 블록체인(Blockchain)

##### 가. 탄생의 배경

사람들이 이용하는 대부분의 서비스에서는 다양한 데이터가 생성됩니다. 이러한 데이터 중에서 금융 거래 정보를 한 곳에 모아 두게 되는데, 이를 클라우드 서비스라고 합니다.

시스템을 악의적인 사용자로부터 방어하는 기술은 매우 중요합니다. 금융 거래 정보처럼 중요한 데이터의 경우에는 데이터를 어떻게 보관하고 관리하는지가 매우 중요한 문제입니다.

블록체인 기술은 이러한 보안 문제를 혁신적으로 대비하기 위해 등장했으며, 위험성을 해결하기 위해 활용되고 있습니다.

### #2

##### 나. 정보 저장 기술

블록체인은 데이터를 중앙에 보관하는 클라우드 서비스와는 정반대의 개념입니다. 거래 등으로 생성된 각종 데이터를 사용자들이 각자 보관하고 있는 방식이며, 자료를 보관하는 방식입니다. 즉, '정보 저장 기술'입니다.

##### 다. 저장의 형태

정보를 하나의 중앙집중형 서버에 저장하는 것이 아니라 분산형으로 저장합니다. 블록체인은 분산형 데이터베이스와 유사한 형태로 데이터를 저장하는 연결 구조체 리스트를 말합니다. 블록체인에 참여한 모든 구성원이 네트워크를 통해서 데이터를 검증하고 저장함으로써 특정인이 임의대로 조작하기 어렵게 설계된 저장 플랫폼이라고 할 수 있습니다.

### #3

#### 2. 블록의 생성 원리

#### 가. 분산장부 기술

거래 정보의 검증을 위해 10분 동안에 발생한 거래를 모아 묶은 형태를 블록(Block)이라 하고, 그 블록들이 순차적으로 사슬처럼 연결(Chain)된다는 의미에서 블록체인이라고 불립니다. 다시 말하면 블록이란, 발생한 비트코인 거래를 약 10분 단위로 묶은 것이며 채굴이 일어나는 단위를 말합니다. 블록체인이라는 명칭처럼 거래 내역을 담은 신규 블록이 형성되어 기존 블록에 계속 연결(Chain)되는 구조적 특성에 기인합니다. 블록체인(Blockchain)은 당사자간의 거래 정보를 네트워크에 참여하는 모든 구성원이 공동으로 보관 및 저장하는 ‘분산장부(Distributed Ledger)’ 기술입니다.

#### #4

##### 나. 기술 구조

블록체인은 블록(Block)들로 구성되어 있으며, 각 블록은 다시 헤더(Header)와 바디(Body)로 구성되어 있습니다. 바디에는 거래별 트랜잭션(Transaction)이 기록되어 있습니다. 여기서 헤더는 해쉬(Hash)값과 논스(Nonce)를 포함하고 있습니다. 해쉬값은 현재 블록을 이전 블록과 다음 블록으로 연결하는 역할을 합니다. 논스는 암호화된 시스템에서 사용되는 임의의 수를 말합니다. 블록체인의 참여자들은 해쉬값을 이용하여 해당 데이터의 정합성을 검증할 수 있습니다.

#### #5

질문자: 비트코인은 무엇인가요?

전문가: 비트코인은 블록체인 기술을 활용한 첫 번째 성공 사례이며, 은행 등과 같은 신뢰할 만한 기관이 없는 최초의 P2P 암호화폐 시스템입니다. 블록체인, 작업증명, 롱기스트 체인(Longest Chain)의 합의를 통한 메커니즘으로 12.5 BTC를 제공합니다. 시장에서 가장 많은 거래가 이루어지는 가상화폐로서 그 의미가 있습니다.

#### #6

##### 3. 블록체인의 거래

##### 가. 블록체인의 거래 프로세스

- ① 거래 당사자들이 거래를 시행할 때 해당 거래 정보가 블록체인 네트워크상의 모든 참여자에게 전송됩니다.
- ② 블록체인 참여자들은 거래 정보를 전송받고, 상호 검증을 통해 암호화된 거

래 정보가 타당한지 여부를 판단합니다. 이와 같이 구성원 간의 유효성 검증을 통해 타당성이 입증된 거래 정보만 신규 블록에 저장됩니다.

③ 기존의 블록에 신규 블록이 연결되어 하나의 블록체인을 구성하게 되고, 당사자 간의 거래가 성공적으로 완료됩니다.

## #7

### 나. 블록체인의 거래 원리

블록체인은 현재까지 발생한 원장 거래를 시간 순서대로 기록한 것이며, 네트워크상의 모든 참여자에게 공개된 공공원장입니다. 블록체인 기술을 적용한 대표적인 분야는 암호화폐 거래이며, 비트코인을 비롯한 대부분의 암호화폐 거래에 활용되고 있습니다. 암호화폐의 거래 과정은 탈중앙화된 전자장부에 기록되며, 블록체인을 기반으로 실행되는 많은 참여자들의 각 컴퓨터에서 서버가 운영되기 때문에 중앙은행이 없음에도 개인과 개인 간의 자유로운 거래가 가능합니다.

## #8

### 다. 블록체인 관리

블록체인에서는 중앙 서버나 관리하는 직원이 없어도 거래 장부를 모든 사용자가 나누어 보관하고 계속 새로운 거래가 발생할 때마다 업데이트를 합니다. 이 기술을 응용하여 만든 것이 바로 비트코인입니다. 비트코인은 10분마다 하나의 블록에 거래 내역을 저장하고, 새로운 블록을 연결(Chain)하여 디지털 거래 장부를 생성합니다. 거래 장부인 블록들이 체인처럼 얹혀 있어 위조가 불가능하게 설계되어 있습니다.

### 라. 블록체인의 분류

블록체인은 트랜잭션의 기록 및 관리(블록 형성)가 가능한 개방형(Public) 블록체인과, 허가를 받은 경우에만 네트워크에 접속이 가능한 폐쇄형(Private) 블록체인으로 구분합니다.

## #9

### 4. 블록체인의 특징

#### 가. 공동 유지 관리

블록체인은 모든 노드가 공동으로 시스템의 유지 관리를 수행합니다. 신규 블록이 생성될 때 참여자들이 기존에 가지고 있던 장부들과 전부 비교하는 작업

을 실행합니다. 이를 통해 그 내용이 상이한 경우 해당 블록은 시스템에 등록되지 못합니다. 따라서 장부를 조작하기 위해서는 새로운 블록이 연결되기 전에 모든 사용자의 저장 장소(컴퓨터)를 해킹해야 하는데 블록체인이 수시로 갱신되기 때문에 사실상 장부의 조작이 불가능합니다.

#### #10

##### 나. 탈중앙화

블록체인 플랫폼의 가장 큰 특징은 중개기관이 없다는 점입니다. 즉, 전통적인 시스템과 구별되는 가장 큰 차이는 신뢰를 담보해 주는 '제3의 기관(Trusted Third Party)'이 존재하지 않는다는 것입니다.

- 전체 시스템을 제어하는 단일 노드(제3의 기관)가 없습니다.
- 모든 노드의 권리와 의무는 동일하며, 일부 노드에 장애가 있더라도 전체 시스템에는 영향을 미치지 않습니다.

거래 정보를 특정 기관의 중앙 서버의 형태가 아니라 P2P(Peer-to-Peer) 네트워크에 분산하여 참여 구성원들이 공동으로 기록하고 관리합니다. 따라서 신뢰할 수 있는 제3의 기관을 설립하고 운영하기 위한 인력과 자원의 투입이 불필요합니다. 모든 거래 기록은 구성원들에게 암호화되어 공개되기 때문에 거래의 투명성을 제고할 수 있습니다.

#### #11

##### 다. 데이터의 보안

보안 측면에서의 안전성도 상당히 높은 수준으로 유지될 수 있습니다. 해킹 등 정보 유출의 표적이 되는 중앙 서버가 존재하지도 않고, 악의적인 공격자가 블록체인 네트워크 전체를 해킹하거나 조작하는 것은 불가능합니다.

- 전체 시스템의 모든 노드는 완전한 최신의 사본을 저장합니다.
- 단일 노드의 데이터베이스만을 수정하는 행위는 전체에 아무런 영향을 미치지 않습니다.
- 일정한 시간이 지난 거래 기록은 모든 노드에 동일하게 저장됩니다.

#### #12

##### 라. 상호 신뢰성(투명성)

시스템의 안정성도 높다고 평가받고 있습니다. 왜냐하면, 일부 참가자의 시스

템에 오류가 발생하더라도 전체 네트워크에 미치는 영향은 매우 미미하기 때문입니다. 블록체인 플랫폼에서는 모든 참여자가 거래 기록의 보관 및 갱신 작업에 참여합니다.

또 일부 노드가 악의를 가진 자에게 점거되더라도 전체 시스템은 신뢰성 있는 거래를 진행할 수 있습니다. 전체 시스템의 데이터베이스가 투명하게 공개되어 있기 때문에 모든 사람을 속일 방법이 없습니다.

따라서 기존의 중앙집중형 시스템에 비해 효율성(Efficiency), 보안성(Security), 시스템의 안정성(Resilience), 투명성(Transparency)의 측면에서 장점을 가지고 있습니다. 한편, 신뢰를 담보해 줄 외부기관이 존재하지 않기 때문에 블록체인 시스템에서 자체적으로 신뢰를 형성하는 메커니즘이 요구됩니다.

#### #13

##### 5. 블록체인 기술이 제공하는 환경

###### 가. 데이터베이스 민주주의 환경의 제공

디지털 환경에서 신뢰 프로세스를 구현할 수 있습니다.

###### 나. 정보의 통제권

개인정보의 통제권을 개인에게 제공한다는 점에서 기존의 체계를 파괴할 수 있는 잠재력을 내포하고 있습니다.

###### 다. 제3자의 제거

블록체인은 모든 정보를 수집하고 관리 및 검증하는 중재자를 제거함으로써 디지털 세상에서 경제적 활동과 사회적 활동을 더욱 민주화하는 기술을 제공합니다.

인증과 안정성의 확보 등의 중재자 역할을 합니다. 또 거래를 연결해 주는 서비스 등 관련 비즈니스에 커다란 파급력을 제공할 수 있는 탈중재자 및 중재기관의 형태를 보유합니다. 또 공급사슬 내의 정보가 공급사슬 참여자 모두에게 공유되는 것이 가능합니다.

#### #14

##### 6. 블록체인 기술의 직접 효과

블록체인은 참여자가 열람할 수 있는 디지털 장부(분산원장)를 활용하고 있습니다. 일반적으로 공유되고 공개된 자료는 조작이나 왜곡이 어렵습니다. 디지털 장부를 이용하는 블록체인은 변조나 왜곡을 방지하기 위해 생성되는 자료들을 참여자가 보관하고 있는 장소에 분산하여 저장합니다.

그래서 악의적인 목적을 가지고 해킹을 시도하는 경우에는 분산되어 있는 모든 자료를 해킹해야만 목적을 달성하기 때문에 데이터의 위·변조나 정보 왜곡의 위험이 크게 줄어들게 됩니다. 일반적으로 현재 사회에서 기대할 수 있는 블록체인 기술의 직접적인 효과는 다음과 같습니다.

#### #15

가. 제3자 플랫폼의 존재 가치가 없음

- ① 블록체인의 도입으로 인해 거래 활동을 지원하던 중간관리자나 인증을 담당하던 중앙기관과 같은 제3자 플랫폼의 존재 가치가 없어집니다.
- ② 분산화를 통해 공식적인 인터넷 플랫폼이 없더라도 신제품이나 서비스를 제공할 수 있는 스타트업 기업의 진출 가능성이 증가합니다.

나. 자산에 대한 가치평가 방식과 교환 과정의 변화를 제공

- ① 블록체인은 자산에 대한 가치평가 방식과 교환 과정에서 커다란 변화를 가져옵니다.
- ② 암호화폐 기술은 어떠한 형태의 자산도 복제하거나 이중으로 결제할 수 없으며 가치평가를 용이하게 합니다. 그 결과 시장에 영향력을 미치게 됩니다.

다. 기업 간의 계약과 이행, 파트너십의 관리 및 거버넌스가 가능

- ① 스마트 계약 기술 등을 통해 사람의 직접적인 개입이 없이 기업 간의 계약을 체결하고 이행할 수 있습니다. 또 파트너십의 관리와 거버넌스가 가능합니다.
- ② 블록체인에 저장된 공통의 공유 데이터를 활용하여 기업 간의 계약에서 이견 및 문제 제기 등을 줄일 수 있습니다. 또 신뢰 형성을 통해 계약 대상의 범위가 확장됨에 따라 시장의 규모 또한 커질 수 있습니다.