

제 4 장. 블록체인

학습목표
<ul style="list-style-type: none">▪ 학습내용: 해당 차시에서 학습할 학습주제(목차)를 제시해 주세요.▪ 학습목표: 해당 차시 학습을 통해 <u>학습자들이 달성해야 할 목표</u>를 학습내용과 연계하여 작성해 주세요.

▶ 학습내용

1. 블록체인이란?
2. 블록체인의 발전 과정
3. 블록체인 활용 사례
4. 블록체인의 분류

▶ 학습목표

1. 블록체인을 이해하고 설명할 수 있다.
2. 블록체인의 발전과정을 이해하고 설명할 수 있다.
3. 블록체인 활용 사례에 대해 알 수 있다.
4. 블록체인의 분류하고 설명할 수 있다.

1.블록체인이란?

2008년 10월31일 저녁, 사토시 나카모토 라는 사람이 암호화 기술 커뮤니티 메인에 ‘비트코인 : P2P 전자화폐 시스템’ 이라는 논문을 올렸다. 이 논문에서 사토시 나카모토는 비트코인을 “전적으로 거래 당사자 사이에서만 오가는 전자화폐” 라고 소개하고 P2P(Peer to Peer) 네트워크를 이용해 이중 지불을 막는다“라고 설명했다. 사토시 나카모토가 말한 ‘P2P 네트워크를 이용해 이중지불을 막는 기술’이 바로 ‘블록체인’이다. 이중지불이란 돈을 두 번 쓴다는 말이다. 전자화폐는 지폐처럼 물리적인 실체 없이 그저 컴퓨터상에 데이터로만 존재하기 때문이다. 데이터는 쉽게 복제할 수 있다. 원본과 사본에도 차이가 없다. 컴퓨터 파일을 복사하듯 돈을 복제해낼 수도 있다는 뜻이다.

무한정 복제할 수 있는 돈은 가치가 없다. 따라서 전자화폐를 돈으로 쓰려면 데이터를 함부로 고칠 수 없도록 장치를 해둬야 한다. 블록체인 안에는 이런 장치가 심어져 있다. 이 점이 비트코인을 혁명적인 기술로 만든 가장 큰 특징이다.

블록은 비트코인 장부를 말한다. 블록은 10분마다 하나씩 만들어지는데 언제, 누가, 누구에게 얼마의 비트코인을 보냈는지를 모두 기록하고 있다. 이 블록들은 시간 순서에 따라 ‘해시’로 체인처럼 꿰어 있다. 이렇게 ‘해시’로 연결되어 있어 블록체인이라고 한다. 모든 참여자들이 블록체인은 위조나 변경이 불가능에 가깝다고 하는데 그 이유는 10분마다 하나의 암호화된 블록이 형성되어 블록 위에 쌓아 올려지기 때문이다.

‘해시’라는 단방향 암호화 알고리즘을 사용해 새 블록을 만들기 위한 경쟁 속에서 생성에 성공한 컴퓨터에서 보상으로 지급되는 것이 비트코인이다. 또한 블록 생성에 참여하는 것을 채굴 즉, 마이닝 (Mining)이라고 한다.

사토시의 논문에는 블록체인이라는 용어가 없다. 블록체인은 ‘블록들이 체인처럼 연결되어 있다’ 해서 붙여진 명칭인데, 사토시가 ”chain of hash based proof-of-work“라고 표현한 것을 간단하게 블록체인이라 명명한 것이다. 즉 ‘해시암호 기반의 작업증명’ 이 블록인 셈이다. 이렇게 비트코인과 블록체인은 다른 차원의 개념이다. 비트코인은 시스템의 명칭이고, 블록체인은 그 시스템을 설계한 알고리즘이다.

2. 블록체인의 발전 과정

1)블록체인의 기본 용어 정리

①블록 (Block) : 데이터를 저장하는 단위로 바디(Body)와 헤더(Header)로 구분된다. 바디에는 거래 내용이, 헤더에는 머클해시나 논스(Nounce: 암호화와 관련되는 임의의 수)들의 암호코드가 담겨 있다. 블록은 약 10분을 주기로 생성되며, 거래기록을 끌어모아 블록을 만들어 신뢰성을 검증하면서 이전 블록에 연결하여 블록체인 형태가 된다.

②블록체인 (Blockchain): 블록에 데이터를 담아 체인 형태로 연결, 수많은 컴퓨터에 동시에 이를 복제해 저장하는 분산형 데이터 저장 기술이다. 공공 거래 장부라고도 부른다. 중앙 집중형 서버에 거래기록을 보관하지 않고 거래에 참여하는 모든 사용자에게 거래 내역

을 보내 주며, 거래 때마다 모든 거래 참여자들이 정보를 공유하고 이를 대조해 위조나 변조를 하라 수 없도록 되어있다.

③분산원장 : 분산된 P2P 망 내 참여자들이 모든 거래 목록을 지속적으로 갱신하는 디지털 원장으로 중앙관리자나 중앙 데이터 저장소가 없으며 P2P망 내 모든 참여자(Peer)가 거래 장부를 서로 공유하여 감시 관리하기 때문에 장부의 위변조가 불가하다.

④해시(Hash): 해시는 하나의 문자열을, 이를 상징하는 더 짧은 길이의 값이나 키로 변환하는 것이다. 해시와 암호화는 다른 개념인데, 암호가 정보를 숨기기 위한 것이라면 해시는 정보의 위변조를 확인하기 위한 방법이다.

대칭 및 비대칭 암호화 기법과 함께 해시를 사용함으로써 전자서명, 전자봉투, 전자화폐 등 다양한 전자상거래를 위한 기능을 구현할 수 있다.

⑤해시함수 : 어떤 데이터를 입력해도 같은 길이의 결과를 도출하는 함수이다. 도출되는 결과가 중복될 가능성이 낮고, 결과값으로 입력값을 역으로 추정하기 어렵다. 이 때문에 해시값을 비교하면 데이터의 변경이 발생했는지 파악할 수 있다.

⑥노드(Node) : 일반적으로 네트워크에서 노드란 연결 지점을 말하며, 다른 노드로의 데이터 전송을 인식하고 처리하거나 전달할 수 있도록 프로그램되어 있다. 컴퓨터 네트워크에서 물리적 노드란 네트워크에 붙어서 전송할 정보를 만들고 통신채널 상으로 이를 주고받는 활성화된 전자 기기를 일컫는다.

⑦논스(Nonce): 논스는 블록을 연결하기 위한 작업증명에 쓰인다. 새 블록이 만들어졌을 때, 논스 값이 비어있다. 난이도 목표를 만족하는 논스를 찾으면 해당 블록은 유효한 것으로 인정되고 체인으로 연결된다.

⑧채굴 : 암호화폐의 거래내역을 기록한 블록을 생성하는 대가로 암호화폐를 얻는 행위를 말한다.

⑨이중지불 : 단일 화폐 단위가 두 번(이중) 결제되는 것

은행의 경우 중앙제어 시스템이 있기 때문에 거래 요청이 발생한 순서대로 거래를 진행하면 이중 지불 문제가 발생할 수 없다. 블록체인은 작업증명 방식의 합의 알고리즘을 이용하여 이중지불 문제를 해결하였다.

⑩작업증명(Proof of Work-PoW): P2P네트워크에서 일정 시간 또는 비용을 들여 수행된 컴퓨터 연산 작업을 신뢰하기 위해 참여 당사자 간에 간단히 검증하는 방식, 또는 블록체인에서 정보를 랜덤한 논스 값과 해시 알고리즘을 적용시켜 설정된 크기의 해시보다 작은 값을 도출하는 과정으로, 새로운 블록을 블록체인에 추가하는 작업을 완료했음을 증명하는 것이다.

❶지분증명(Proof of Stake-PoS) :알고리즘의 한 형태로서 이를 통해 암호화폐, 블록체인

네트워크가 분산화된 합의를 얻는 것.

❷스마트 컨트랙트(Smart Contract): 디지털로 계약서 작성, 제3자 없이 정해진 대로 스스로 조건이 실행되는 계약이다.

❸가상화폐 공개 -ICO (Initial Coin Offering) : 사업자가 블록체인 기반의 암호화폐 코인을 발행하고 이를 투자자들에게 판매하여 자금을 확보하는 방식.

❹암호화 : 의미를 알 수 없는 형식으로 정보를 변환하는 것

❺하드포크 (Hard fork): 기존의 블록체인과 호환되지 않는 새로운 블록체인에서 다른 종류의 가상화폐를 만드는 것을 말한다.

2) 블록체인 1.0

초기 블록체인의 개념은 2009년 나카모토 사토시의 P2P 논문에서 발표된 내용을 블록체인 1.0 이라고 하며, 이는 기본적으로 공유 블록체인의 특징을 가지고 있다. 누구든지 거래내역을 볼 수 있고, 누구나 네트워크의 참여자가 될 수 있다. 화폐 목적으로 제한되어 사용되었기 때문에 투명성과 보안 측면에 가장 큰 중점을 둔 것이 특징이다.

우리가 블록체인에 대해 특징적으로 기억하는 대부분의 것들이 비트코인의 블록체인 개념에서 만들어졌다. 블록체인 1.0에서 만들어진 개념인 ‘분산원장을 통한 보안’의 강점은 다음 세대로 넘어가면서도 지속되었다. 이는 향후에도 지속될 개념 정립이 초기에 이루어졌다는 점에서 큰 의미가 있다.

3)블록체인 2.0

비트코인의 문제점을 해결하고자 스마트 컨트랙트를 도입한 블록체인 2.0이 탄생하게 된다.

대표적인 이더리움은 계약을 통해 특정 조건을 설정하고 조건 이행시 해당계약이 이행되게 하는 기능을 할 수 있다. 비탈릭 부테린(Vitalik Buterin) 이 2014년 개발한 가상화폐로 블록체인 기술과 스마트 컨트랙트가 적용되어 있어 각광받는 가상화폐 중 하나이다. 블록체인 기술은 가상화폐로 거래할 때 발생할 수 있는 해킹을 막는 기술로 거래에 참여하는 모든 사용자에게 거래 내역을 보내어 거래 때마다 이를 대조하여 데이터 위조를 막는 방식을 사용한다. 스마트 컨트랙트는 미리 지정해 놓은 특정한 조건이 일치될 경우 자동으로 계약이 실행되는 프로그램이다.

스마트 컨트랙트는 제 3자를 거치지 않고 신뢰가 없는 당사자끼리 미리 프로그래밍 된 규칙에 따라 특정 조건이 달성되면 자동적으로 프로그램이 실행되어 이행되는 계약이라고 볼 수 있다. 이를 기반으로 수많은 형태의 파생 서비스를 만들 수 있는데 이러한 서비스를 분산 어플리케이션이라고 한다.

일반적으로 암호와 통화 업계에서는 블록체인 기술의 통화 이외의 분야에의 응용은 비트코인 2.0 또는 블록체인 2.0 이라고 부른다.

블록체인 2.0의 대표적인 이더리움은 2세대 블록체인으로 불리며 블록체인 기술을 여러 분야에 접목할 수 있도록 업그레이드한 것이 특징이다. 기존 블록체인인 시스템을 금융 거래 이외의 모든 분야로 확장하는 플랫폼이 되었다. 이더리움은 거래기록뿐 아니라 스마트 계약 기능을 통해 계약서, SNS, 이메일, 전자투표 등 다양한 어플리케이션을 투명하게 운영할 수 있는 확장성을 제공한다. 즉 이더리움 플랫폼 위에서 분산형 어플리케이션 D-App(Decentralized App)을 만들 수 있는 것이다. 실제로 이더리움 이후 많은 D-App들이 개발되었고 거대한 블록체인 생태계를 형성하게 된 것이다. 이더리움 로드맵을 보면 하드포크에 따라 4단계로 나누어 표현한다.

①1단계 ‘프론티어(Frontier)’는 가상화폐 거래를 위해 코인을 채굴 및 발행하고 네트워크를 형성하는 단계이다.

②2단계 ‘홈스테드 (Homestead)’는 이더리움의 성장을 위해 각종기능을 업데이트하고 보완하는 단계이다.

③3단계 ‘메트로폴리스 (Metropolis)’는 이더리움의 대중화를 위한 시기이며, 이더리움의 본격적인 활용이 기대되는 시기이다.

④4단계 ‘세레니티 (Serenity)’는 이더리움의 최종단계이며, 전 세계에 발생하는 대량의 모든 기록을 담을 정도의 블록체인이 완성되는 시기이다.

4)블록체인 3.0

블록체인 3.0은 폭넓은 적용과 스마트 컨트랙트의 발전이라고 말할 수 있다.

블록체인 3.0에 대한 명확한 정의는 아직까지 존재하지 않는다. 다만 지금까지의 블록체인이 금융과 계약, 그리고 화폐의 가치에 한정되어 사용되어 온 것과 달리 향후에는 지금보다 더 많은 정보를 블록체인 상에 기재하고 더욱 정교화된 스마트컨트랙트가 도입되어 우리의 생활에 긍정적인 영향을 줄 것이다. 또한 이는 헬스, 교육, 사회, 보건, 문화, 공유경제, 기술분야에 모두 녹아들어 진정한 초연결사회로 가는 첫걸음이 될 가능성이 높다.

실제로 블록체인 3.0과 비전을 같이 하는 다양한 DAPP (탈중앙화된 어플리케이션)과 플랫폼이 등장하고 있다. 그 간에 블록체인 자체의 기술적인 성숙도 있었다. 컴퓨팅 파워 과다 소모, 느린 거래속도 등 블록체인에 제기됐던 여러 한계점을 극복하고 있는것이다.

블록체인 3.0은 사회 전반에 기술이 적용되는 기술로써 인터넷을 다양하게 쓰는 것처럼 생활패턴이 자연스러워지고 사회 전체에도 또 한 번의 변화를 가져올 것이다. 또한 처리시간 지연의 문제점을 해결하기 위해 합의 알고리즘의 변화, 분산 장부관리 기술의 등장과 하드포크 방지를 위해 블록체인 내 자체 의사결정 합의 기능을 탑재한 플랫폼이 대두될 것이다.

3. 블록체인 활용 사례

1) 관세청

관세청이 주도하는 개인통관 블록체인 시범사업으로 기존 12시간 이상 소요되던 통관처리 방식이 블록체인을 통해 실시간으로 처리되는 시스템으로 변경된 것이다.

과기부와 관세청이 협력한 ‘전자상거래물품 개인통관 시범서비스’는 전자상거래업체의 주문정보와 운송업체의 운송정보를 블록체인에 실시간으로 공유하고 시범 사업을 통해 통관 자동화로 취합해 정리하여 서류의 위·변조 위험과 통관에 필요한 시간을 단축할 수 있게 된다. 따라서 현재 늘어나고 있는 개인의 소량 해외 직구 물품에 대한 신고 시간과 비용을 단축할 수 있을 것으로 기대된다.

배송업체와 전자상거래업체의 데이터를 블록체인 장부를 통해 동시 확인, 수차례 엑스레이 검사를 진행했던 과거와 달리, 통관처리가 간소화되는 것이다. 이를 통해 일 평균 3만 6천 건에 그쳤던 통관처리량도 급증할 전망이며, 1건당 약 5일 이상 걸렸던 통관절차도 2일 이내로 줄어들고 있다.

2) 농림축산식품부

사육장과 도축장, 가공장, 판매장의 데이터를 블록체인으로 묶어 축산물 유통과정에서 문제가 발생할 시 추적 기간을 기존 6일에서 10분 이내로 단축시킨다. 이것을 블록체인과 IOT를 활용한 사례이다. IOT 디바이스로 수집된 정보를 블록체인에 자동으로 입력하고 쇠고기 유통 단계별 이력 정보와 증명서를 블록체인에 저장, 공유하는 시스템을 구축한 것으로 기존 시스템에서 쇠고기 이력 신고 규정은 5일 이내였는데 신고전에 문제가 발생할 시 조회가 어려운 한계점이 있었다. 블록체인과 IOT를 이용하면 실시간으로 유통 경로를 추적할 수 있어서 이런 한계점을 해결할 수 있다.

3) 국토교통부

국토교통의 부동산 거래 블록체인 시범사업은 토지대장을 국토부와 지자체, 금결원이 함께 보유해 민원인이 부동산 담보 대출 시 은행 방문으로 원스톱 처리가 가능하도록 만든 것이다. 이전에는 부동산을 매매하거나 혹은 대출하는 경우 은행, 국세청 등에 종이로 된 부동산 증명서를 제출했다. 이 경우 종이 증명서는 위·변조가 가능해서 범죄에 악용되는 경우가 있었다. 그러나 블록체인 기술을 활용할 시 부동산 정보를 데이터 형식으로 실시간으로 공유할 수 있어 위와 같은 문제점을 해결할 수 있을 뿐만 아니라, 사용자가 증명서를 발급받는 데 걸리는 시간을 단축할 수도 있다. 2019년 1월부터 제주도 내 11개 금융기관에서 시범 운영되고, 추후 ‘부동산 거래 통합 서비스’로 확대 개편 운영되고 있다.

4) 중앙 선거관리위원회

중앙선거 관리 위원회의 온라인 투표 블록체인 시범사업이 진행되었다. 중앙선관위는 2013년부터 온라인 투표 시스템 ‘케이보팅(K-voting)’을 운영해오고 있었다. 그러나 온라인 투표는 해킹과 조작의 위험이 있어 중요성이 큰 선거에는 이용되지 못했다. 하지만 위 변

조가 어려운 블록체인 기술을 기반으로 온라인 투표 시스템을 구축한다면 이런 한계점을 극복할 수 있다. 또한 쉽고 간편한 투표 참여로 투표율을 증가시킬 수 있으며 비용 절감 효과도 있다.

투표 블록체인 네트워크를 구성, 유권자가 본인인증을 거치면 후보자와 참관인, 선관위가 모두 투명하게 투표 결과를 검증할 수 있다. 정부는 정당 등 온라인 투표를 희망하는 곳에 관련 시스템을 공급할 계획이다.

5)외교부

외교부는 2019년부터 국가 간 전자문서 유통에 블록체인 기술을 활용하고 있다. 기존에는 공문서 등 국내 문서를 해외에서 사용하기 위해 내용 확인에만 14일이 걸렸으나, 일부 공문서를 블록체인으로 올려 해외에서의 행정 처리가 간소화된다는. 실시간으로 문서의 발급 사실과 내용을 알 수 있다.

6)해양수산부

해양수산부의 블록체인 시범사업은 컨테이너 관리와 운송 업무에서 이뤄진다. 과거에는 컨테이너 반출에 일일이 별도의 확인이 필요했으나, 2019년부터는 개별 컨테이너 이동시 발급되는 다수의 잔자원장을 블록체인으로 공유해 화주와 터미널, 운송사의 업무 효율이 높아지게 된다. 타 부두 환적 시 필요한 정보를 블록체인상에 저장하여 선사, 운송사, 터미널 간에 공유가 가능하다. 환적 과정을 실시간으로 투명하게 공유하여 업무량과 대기시간을 줄여 효율성을 증대시킬 수 있다.

4. 블록체인의 분류

1) 퍼블릭 블록체인 (Public Blockchain)

퍼블릭 블록체인은 모두에게 개방되어 누구나 참여할 수 있는 형태로 비트코인, 이더리움 등 가상통화가 대표적이다. 주로 정부에서 관리라는 플랫폼이다.

퍼블릭 블록체인 시스템 유지의 핵심은 암호화폐이다. 암호화폐가 없는 블록체인 시스템은 구성은 될지라도 작동이 되지 않는 깡통에 불과하다. 블록체인이 자동차라면 암호화폐가 연료가 되는 것이다. 또한 퍼블릭 블록체인과 암호화폐의 관계는 기술적인 문제가 아닌 경제적인 문제로 보아야 한다. 블록체인은 중앙시스템이 없다. 따라서 각 참여자 (Node)들이 연결되어 자동으로 시스템이 작동되어야 한다. 하지만 보상이 없다면 참여자들은 블록체인의 구성을 위한 자원을 공짜로 공급하지 않을 것이다.

기본적으로 블록체인은 모두 거래기록을 모든 블록에 기록하며 거래에 대한 신뢰를 확보해야 한다.

퍼블릭 블록체인을 사용하는 이유는 블록체인의 가장 큰 장점인 해킹에 대한 안전성이다. 여기서 말하는 해킹은 거래소를 말하는 것이 아니다. 즉, 개인의 해킹이 아니라 장부의 기록을 조작하는 해킹은 궁극적으로 가치를 무효화 시킨다. 이렇게 해킹당한 코인은 아무도 보유하려 들지 않기 때문에 곧 사라지게 될 것이다.

퍼블릭 블록체인은 아이디어가 풍부하고 기존의 기업들을 역전하고 싶어하는 스타트업 기업들이 사용할 수 있다.

2) 프라이빗 블록체인 (Private Blockchain) : 단일 조직, 그룹만이 참가한다.

프라이빗 블록체인은 기관 또는 기업이 운영하며 사전에 허가받은 사람만 사용할 수 있다. 참여자 수가 제한되어 있어 상대적으로 속도가 빠르다. 프라이빗 블록체인으로 하면 회사에서 데이터를 제어할 수 있고 노드를 회사에서만 유지하기 때문에 해킹의 위험에 비교적 안전하다.

프라이빗 블록체인은 서버를 증설하고 유지하는데 거부감이 없는 기업들이 사용할 수 있다.

암호화폐의 블록체인에 기록된 대부분의 정보는 모든 참여자가 열람 가능한 공개 장부이다. 하지만 세상에는 공개되지 않아야 하거나, 일부에게만 공개되어야 하는 정보가 있다. 이런 비공개 정보는 블록체인상에 기록되어선 안된다. 그렇기 때문에 프라이빗 블록체인이 등장하게 된 것이다. 접근이 허락된 참여자에 한하여 사용이 가능하다. 소수의 참여자로 구성된 블록체인이므로 보증된 신원의 참여자들만 정보 접근이 가능하므로 경쟁적 합의 알고리즘이 필요하지 않다.

프라이빗 블록체인은 금융권이 가장 큰 관심을 가지고 개발해 나가고 있다.

3) 컨소시엄 블록체인 (Consortium Blockchain)

컨소시엄 블록체인은 중앙관리자가 존재하는 블록체인은 블록체인의 중요가치인 탈중앙화 정신에 위배 되어 진정한 블록체인이 아니라는 의견 때문에 등장하게 된 것이다. 컨소시엄 블록체인은 특정 참여자만 참여할 수 있는 프라이빗 블록체인과 유사한 개념이다. 컨소시엄 블록체인은 여러 집단의 협의체로서 참가해 신뢰성과 익명성을 높이는 방식이다. 퍼블릭 블록체인과 프라이빗 블록체인의 단점을 극복하기 위해 나타난 유형인 것이다, 참여자 간의 협의가 필요한 서비스에서는 컨소시엄 블록체인이 주로 사용된다. 특히 금융권은 컨소시엄 블록체인 활용의 대표적인 예라고 할 수 있다. 금융 기관끼리 협의에 따라 중개 기관을 거치지 않고 서비스를 제공하기 때문에 외환 거래와 증권 거래 등에 컨소시엄 블록체인이 효과적이다.