

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?

은행을 거치지 않아도 전 세계 누구에게나 돈을 직접 전할 수 있다면 가장 좋은 점은 환전과 송금에 드는 수수료를 아낄 수 있다는 것이다. 서버가 필요 없는 클라우드 저장소가 있다면 해커가 공격할 거점이 없어지니 데이터를 더 안전하게 보관할 수 있을 것이다. 관리자가 필요 없는 인터넷 주소 시스템을 가질 수 있는 기술은 어떨까? 이런 모든 일이 가능케 한 핵심 기술이 바로 ‘블록체인’이다.

블록체인은 비트코인에 대해 얘기할 때 가장 많이 언급된다. 은행 없는 글로벌 금융시스템이 바로 비트코인이다. 가상화폐 비트코인은 세상에 나타나서 시가총액으로 세계 100대 화폐 안에 들어갈 정도로 성장했다. 이런 비트코인이 세상에 나올 수 있었던 이유가 블록체인 덕분이다.

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. 이후 2달 후 2009년 1월 3일 사토시는 논문에서 설명한 기술을 비트코인이라는 가상화폐로 직접 구현해 보여줬다. 사토시 나카모토가 말한 ‘P2P 네트워크를 이용해 이중지불을 막는 기술’이 바로 ‘블록체인’이다. 이중지불이란 돈을 두 번 쓴다는 말이다. 만원짜리 지폐 한 장이 있다고 치자. 이 돈으로 만원짜리 책을 한 권 사면 내 지갑은 텅 빈다. 내게 없는 돈을 마치 있는 것처럼 꾸며댈 도리가 없다. 그런데 그 만원이 전자화폐라면 상황은 달라진다. 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.

과거 블록과의 연결을 ‘체인’으로 비유했는데, 이는 ‘해시’라는 암호 값으로 연결된다. 이 해시값은 거래 내역 정보가 담긴 블록의 데이터가 단 하나라도 바뀌면 해시값 전체가 바뀌게 된다. 예를 들어 과거 거래 내역을 변경하려 한다면, 그 블록의 해시값은 변경되고 과거 블록과 연결되어 있는 블록들 모두 변하게 되는 것이다. 또한 거래 장부를 모든 사람들이 공유하고 대조를 통해 잘못된 거래 내역을 잡아내기 때문에 10분 안에 전 세계 모든 거래자의 거래 내역을 바꾸는 것은 불가능하다. 실제로 전세계에 존재하는 슈퍼컴퓨터의 연산 능력을 다 합친다고 하더라도 해킹은 불가능하고 설령 있다고 하더라도 그 해킹으로 얻는 이득은 없을 것이다.

‘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.

비트코인은 코드라고 볼 수 있는데 블록체인은 눈에 보이지도 않는다. 즉, 비트코인과 블록체인은 한 몸으로 붙어서 태어났는데 비트코인이라는 DAO의 설계자였던 셈이다. 그러다가 분리되기 시작한다.

비트코인의 소스코드는 오픈되어 누구나 공짜로 다운로드해서 실행 할 수 있고 마음대로 응용과 변형이 가능하다. 금융뿐 아니라 온라인 거래를 가능하게 하는 새로운 틀을 개발할 수도 있다. 비트코인이 성공을 거두고 난 뒤 블록체인 기반의 유사 암호화폐들이 쏟아져 나왔고 이들을 ‘알트코인’이라고 통칭한다.

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 내역을 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.

암호화폐는 중앙은행과 같은 발행기관이 없이 거래내역을 기록한 원장을 전 세계 네트워크에 분산저장하게 되는데, 이러한 블록체인을 유지하기 위해 해당 블록을 생성한 사람들에게 일정한 보상을 지급하도록 설계되어 있다. 예를 들어 비트코인의 경우 10분에 한 번씩 새로운 블록이 생성되는데, 이 블록의 이름을 16진수로 표시한 총 64자리의 해시를 찾아내는 사람에게 비트코인을 발행하여 지급한다. 채굴에 성공한 보상으로 지급되는 비트코인의 양은 4년마다 절반으로 줄어드는 반감기를 거친다. 최초의 채굴이 이루어진 2009년에는 50 비트코인을 지급하다가 2013년부터 25비트코인으로 줄어들었고, 2017년부터 12.5 비트코인으로 감소했으며, 2021년에는 6.25개로 줄어들었다. 비트코인은 최종적으로 2140년에 채굴을 중지하도록 설계되어 있다.

가상화폐 채굴 과정에는 높은 연산 능력을 갖춘 컴퓨터가 동원된다. 이 과정에서 그래픽카드가 필요해진다. 과거 그래픽 카드는 컴퓨터 모니터로 화면을 출력하는 용도로 사용되는데 그쳤지만 지금은 고사양 게임이 늘어나면서 이를 구동하기 위한 GPU(그래픽 처리 장치)를 탑재한 그래픽카드가 늘어났다. 고성능 그래픽카드에 탑재된 GPU는 일반 PC의 CPU (중앙처리장치) 능력을 뛰어넘는다. 그래서 대부분 채굴업자들은 PC에 여러 대의 그래픽 카드를 꽂은 채로 채굴에 사용하고 있다. 예전 가상화폐 광풍이 불 당시 그래픽카드 품귀현상이 생긴 이유이다. 수익성이 악화되면서 가상화폐 채굴시장은 양극화가 심해지고 있다. 소수의 대형업체들이 시장을 독식할 수 있다는 우려가 커지는 상황이다. 소수가 시장을 장악하게 될 경우 비트코인의 취약성으로 불리는 '51%의 공격'을 받을 수 있기 때문이다. 이는 비트코인 전체 채굴량의 50% 이상을 보유한 채굴자가 전체 네트워크를 좌우할 수 있다는 것을 의미한다.

'탈중앙화'를 위해 만들어 둔 비트코인 시스템이 이를 충족하는 채굴자의 등장 시점에선 오히려 허점으로 작용할 수 있다는 말이다. 하나의 업체가 50% 이상의 채굴 능력을 보유하게 되면 가상화폐 네트워크 전체를 파괴할 수 있다.

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 이용

하여 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.

⑪지분증명(Proof of Stake-PoS) :알고리즘의 한 형태로서 이를 통해 암호화폐, 블록체인 네트워크가 분산화된 합의를 얻는 것.

지분증명 기반 화폐는 작업증명 알고리즘 기반 화폐에 비해 에너지 사용 측면에서 더 효율적이다.

⑫스마트 컨트랙트(Smart Contract): 디지털로 계약서 작성, 제3자 없이 정해진 대로 스스로 조건이 실행되는 계약이다.

블록체인 계약서를 작성하여, 특정조건 만족 시 계약내용 실행. 대표적 예로 이더리움이 있다.

⑬가상화폐 공개 -ICO (Initial Coin Offering) : 사업자가 블록체인 기반의 암호화폐 코인을 발행하고 이를 투자자들에게 판매하여 자금을 확보하는 방식.

코인이 가상화폐 거래소에 상장되면 투자자들은 이를 사고팔아 수익을 낼 수 있다. 투자금을 현금이 아니라 비트코인이나 이더리움 등의 가상화폐로 받기 때문에 국경에 상관없이 전 세계 누구나 투자할 수 있다.

암호화폐 상장에 성공하고 거래가 활성화될 경우 높은 투자 실적을 기대할 수 있지만 리스크가 매우 크다. ICO가 기업 공개와 다른 점은 공개 주간사가 없고 사업주체가 직접 판매한다는 것이다. 감사가 없고 누구나 자금을 조달할 수 있다. IPO처럼 명확한 상장 기준이나 규정이 없기 때문에 사업자 중심으로 룰을 만들 수 있어 매우 자유롭게 자금을 모집할 수 있다. 그래서 자금 모집 후 사라지는 사기 사례가 빈번히 발생한다.

⑭암호화 : 의미를 알 수 없는 형식으로 정보를 변환하는 것

암호문의 형태로 정보를 기억 장치에 저장하거나 통신 회선을 통해 전송함으로써 정보를 보호할 수 있다. 암호화는 암호기(특정의 비트열)를 사용하여 정보를 암호문으로 변환하는 것이고, 복호화는 복호기를 사용하여 원래의 정보를 복원하는 것을 말한다. 복호기를 갖고 있는 사람 외에는 올바른 정보로 복원할 수 없으므로 복호기가 제 3자에게 알려지지 않으면 정보는 보호된다.

암호체계 또는 방식은 크게 비밀 키 암호 방식과 공개키 암호방식으로 분류된다. 비밀 키 암호 방식은 암호화와 복호화에 동일한 키를 사용한다.

통신할 때에는 송신자와 수신자가 사전에 동일한 키를 비밀로 갖고 있을 필요가 있다. 한편, 공개키 암호방식은 암호화와 복호화에 서로 다른 키를 사용하는데 암호키는 공개하고

복호키는 비밀로 한다.

⑤하드포크 (Hard fork): 기존의 블록체인과 호환되지 않는 새로운 블록체인에서 다른 종류의 가상화폐를 만드는 것을 말한다.

기존 블록체인의 기능개선, 오류정정, 문제점 수정 등을 목적으로 블록체인을 기존의 블록체인과는 호환이 되지 않는 새로운 방식으로 변경한다.

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.

뛰어난 보안성을 지닌 블록체인, 의도적으로 바디 값을 수정해 거래 데이터를 변조하여 이득을 얻으려는 사람이 있다고 가정해보자. 변조를 위해 특정 블록의 바디 값을 수정하면 헤더 안의 바디 데이터를 요약한 머클해시 값이 바뀌게 된다. 이후 해당 블록의 논스를 구하는 작업증명까지 완료하면 해당 블록의 해시값이 변경되는데 이로 인해 다음 블록에 포함되는 해시값 또한 변경된다. 변조를 위해서는 이러한 일련의 과정을 가장 최근에 만들어진 블록까지 반복하고 새로운 블록을 분산시켜 데이터 수정을 정당화해야 한다. 하지만 시간이 지날수록 헤더 안의 나이도 값이 올라가므로 논스를 구하는 시간을 점점 늘어난다.

비트코인의 경우 현재 전 세계에서 가장 성능이 좋은 컴퓨터를 10위까지 모두 가져다가 영향력을 더한다고 해도 변조는 현실적으로 불가능하다. 가장 긴 체인이 가장 안전하다고 이야기하는 이유가 여기에 있다. 이렇듯 블록체인의 안전성은 링크드 리스트를 통한 체인의 길이의 확대와 네트워크 참여자간의 동일한 장부를 통해 생겨난다. 체인의 길이가 길어질수록 이전에 존재하는 하나의 블록을 해팅하는 것은 불가능에 가까워지고 새로이 생겨나는 블록의 거래 데이터를 ‘분산원장’을 통해 모든 노드가 보유하고 있기 때문에 과반수 이상을 수정할 수 있는 연산력을 보유하지 않는 이상 블록체인의 데이터 조작은 불가능하다. 하지만 시간이 지나며 많은 문제점들이 발견되었다. 초기 디자인상의 블록 크기 문제부터, 블록의 합의 과정에서 걸리는 시간, 비싼 송금 수수료, 확장성의 문제까지 초기 화폐의 개념에는 충실했으나 기능적인 면에서는 한계가 존재했다.

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

원래 비트코인의 구조는 특정 관리자가 없고 이중지불을 할 수 없으며, 총공급량이 사전에 결정되어있는 등 통화의 응용을 상정하여 구축되어 있다. 그것을 실현하기 위해 고안된 블록체인의 구조로부터 얻을 수 있는 조작 불능, 검열 내성 등은 통화 이외의 영역에 응용하는 것도 가능하며 인간의 오류를 줄이고 자동화에 따른 비용 절감, 부정의 방지, 투명성 향상 등의 메리트도 얻을 수 있다.

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. 이미 이더리움은 1단계인 프론티어를 넘긴 상태이다. 황무지 상태, 테스트넷을 거쳐 최초 생성된 제네시스 블록 이후 노드가 활성화되는 상태이다. 암호화폐 거래를 위해 코인을 채굴 및 발행하고 네트워크를 형성하는 단계이다.

②2단계 ‘홈스테드 (Homestead)’는 이더리움의 성장을 위해 각종기능을 업데이트하고 보완하는 단계이다. 이더리움 생태계를 구축하는 단계이며 개발자를 위해 각종 기능을 업데이트하고 보완하는 단계로 Pow(작업증명) 합의 알고리즘을 채택하고 채굴과 Dapp의 런칭이 이루어지는 단계이다.

③3단계 ‘메트로폴리스 (Metropolis)’는 이더리움의 대중화를 위한 시기이며, 이더리움의 본격적인 활용이 기대되는 시기이다. 이시기에는 일반인들도 가상화폐를 쉽게 접할 수 있는 시기라 폭발적인 수요가 예상되므로 가상화폐의 채굴방식이 작업증명: PoW(Proof of-Work)에서 지분증명 : PoS(Proof-of-Stake) 방식으로 전환되는 단계이다. 본격적인 활동이 기대되는 시기이다.

④4단계 '세레니티 (Serenity)'는 이더리움의 최종단계이며, 전 세계에 발생하는 대량의 모든 기록을 담을 정도의 블록체인이 완성되는 시기이다. 이 시기에는 채굴방식이 완전히 지분증명 :PoS (Proof -of-Stake)방식으로 전환이 된다.

세레니티로 불리는 이더리움 2.0은 지분증명 알고리즘, 샤딩을 통한 확장성 확보 등 기존 이더리움 보다 다양한 기능을 제공하고 있다.

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.

2017년까지만 해도 블록체인 서비스로 주로 활용된 플랫폼은 이더리움과 비트코인이었다. 즉 블록체인 1.0 혹은 블록체인 2.0 이라고 볼 수 있다. 블록체인 2.0 까지의 블록체인은 여러 산업에 적용하기에는 한계점이 많았다. 이를 보완하고자 아이오타(IOTA), 이오스(EOS), 님(NEM), 리플(Ripple) 등의 블록체인 플랫폼이 등장했다. 이러한 플랫폼이 블록체인 3.0 이다.

2018년부터 국내 블록체인 회사들이 앞을 다투어 우수한 블록체인 3.0 플랫폼을 개발해 나가고 있다. 정부와 지방정부 그리고 대기업들과 벤처기업들까지 블록체인의 활용, 실용화 단계에 와 있는 상황이다. 또한 국내 코인 개발자들은 의료 부분에도 블록체인을 통해 현행 의료시스템의 비효율성을 개선하고자 하고 있으며, 개인의 의료정보를 개인이 소유해 병원 간 구분 없이 진료의 연속성을 갖는 것을 목표로 IOC를 진행하고 있다. 향후 상용화가 된다면 비용 절감 및 진료의 효율화를 모루 이뤄낼 수 있을 것이다. 의료 부분에서 빅데이터와 블록체인의 도입과 실행 또한 기대되는 부분이다.

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

블록체인의 적용사례로는,

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 자동으로 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 전망이다, 1건당 약 5일 이상 걸렸던 통관절차도 2일 이내로 줄어들고 있다.

2) 농림축산식품부

농림축산식품부에서 진행한 축산물 이력 관리 블록체인 사업은 2018년 12월 전북 농가를 시작으로 2019년 전국 지자체로 확대 시행했다. 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 종으로 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. 중앙선거위는 2013년부터 온라인 투표 시스템 ‘케이보팅(K-voting)’을 운영해오고 있었다. 그러나 온라인 투표는 해킹과 조작의 위험이 있어 중요성이 큰 선거에는 이용되지 못했다. 하지만 위 변조가 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 간소화된다. 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.

이외에도 다양한 공공기관, 지방자치단체 등에서 블록체인 플랫폼 구축 사업을 진행하고 있다.

지금은 블록체인 기술의 개발과 더불어 블록체인 기술의 표준화, 플랫폼의 표준화가 절실할 때이다. 현재 표준화가 되어있지 않은 블록체인과 플랫폼들이 연결될 수 있다면 그 시너지는 대단할 것이다.

4. 블록체인의 분류

블록체인은 퍼블릭 블록체인, 프라이빗 블록체인, 컨소시엄 블록체인으로 분류할 수 있다.

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 강통에 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, 개개인의 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.

퍼블릭 블록체인과 프라이빗 블록체인은 참여자의 제한에 차이가 있다 보니 합의 알고리즘에서도 큰 차이를 보인다. 퍼블릭 블록체인의 유지를 위해서는 핵심 합의 알고리즘인 작업 증명과 지분증명 등이 필요하다. 여기서 퍼블릭 블록체인의 한계가 등장한다. 해시파워 경쟁에 따른 과도한 에너지 소모 문제 (예: 채굴을 위해 전기를 많이 사용하는 것)가 발생하는 것이다. 하지만 프라이빗 블록체인은 소수의 참여자로 구성된 블록체인이므로 보증된 신원의 참여자들만 정보접근이 가능하므로 경쟁적 합의 알고리즘이 필요하지 않은 이유이다.

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.