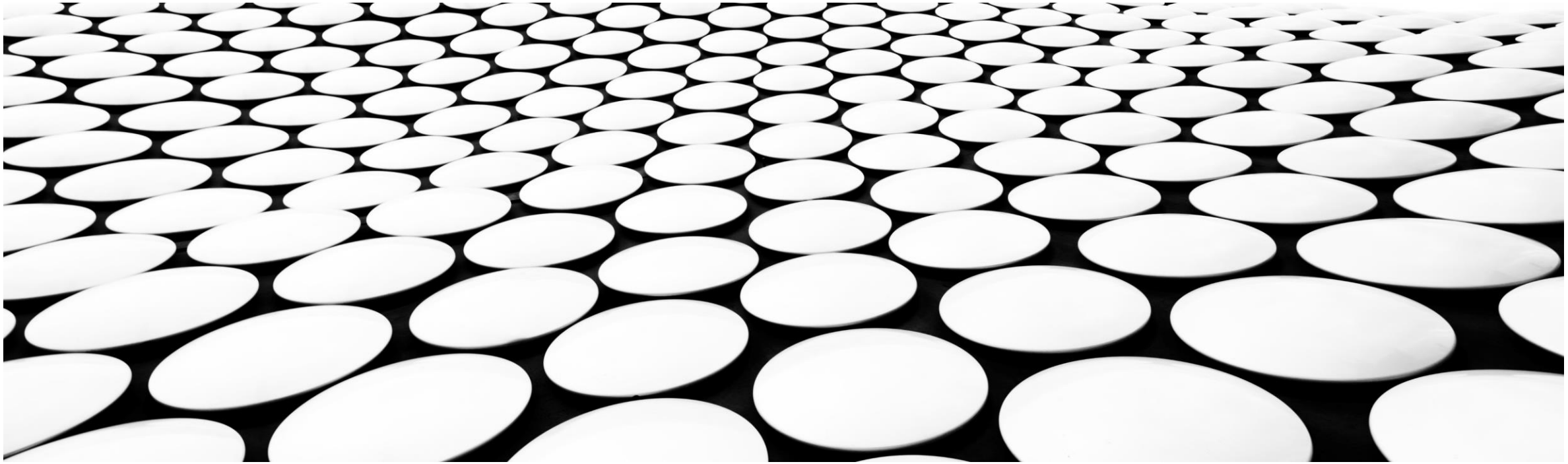
블록체인(BLOCK CHAIN)



지폐와 BITCOIN의 등장

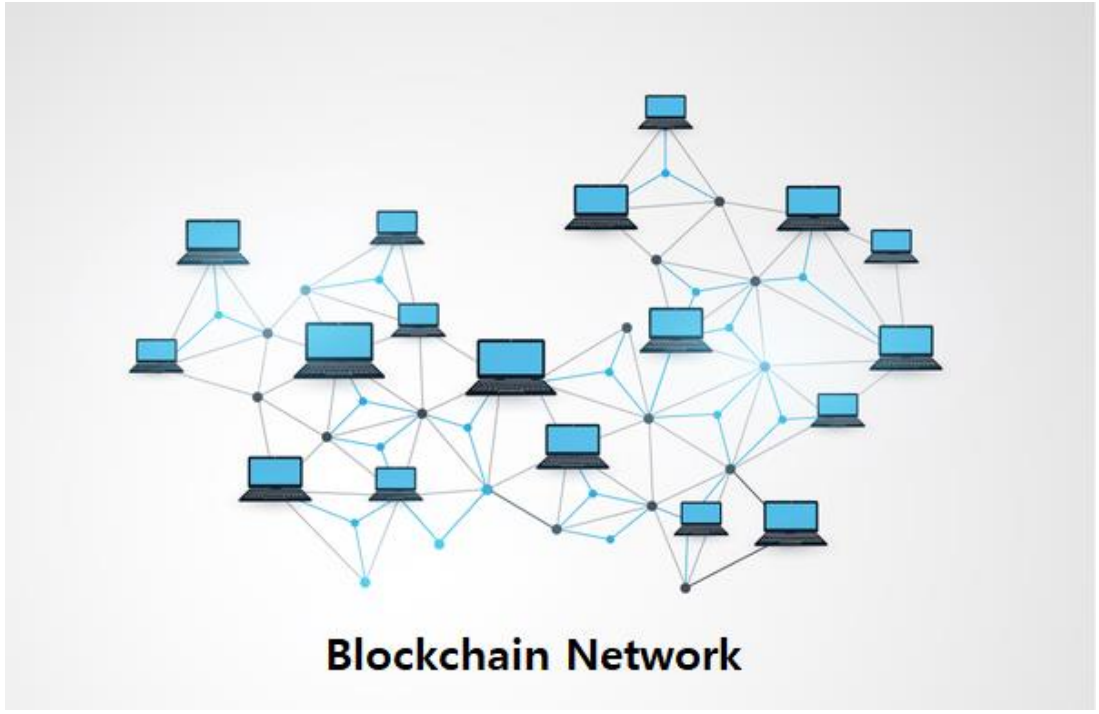
- 세계 최초의 지폐는 **중국 송나라의 교자**이다. 10세기 말경 상인들 사이에서 예탁 증서의 형태로 철화를 대신하는 임시 용도로 발행되었다. 공식적인 지폐의 발행은 1170년 남송 시대에 이르러 상업이 발달하고 화폐의 수요가 늘어난 것이 지폐 발행의 배경이 되었다.
- 영국에서는 영주들이 금을 **은행에 예탁한 금의 가치**만큼 돈을 사용 하였으나, 차후 은행들이 **자신들의 이익을 위하**여 예탁한 금보다 더 영주들에게 돈을 **대출** 해주기 위한 수단으로 지폐(17세기 초 중세 영국에서 발행한 예치증서)를 발행하여 은행의 수익을 위해 발행 하였다.
- 지금의 시대에서는 점점 **플랫폼**화 되가는 과정에서 필요충분 조건을 만족하여 bitcoin이라는 가상의 암호화폐가 등장하게 되고 그것의 가치가 **폭증**하고 있다. 즉 **은행 의존도**에서 벗어나고자 하는 현상이 나타나고 있는 것이다.

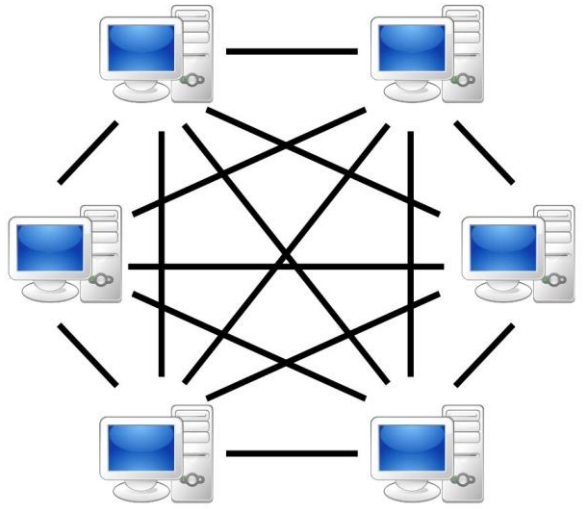
블록체인(BLOCKCHAIN)이란?

- 블록체인이란 **P2P(Peer to Peer)** 네트워크를 통해서 관리되는 **분산 데이터베이스**의한 형태로, 거래 정보를 담은 장부를 **중앙 서버** 한 곳에 저장하는 것이 아니라 **블록체인 네트워크**에 연결된 여러 컴퓨터(**노드**)에 저장 및 보관하는 기술.
- 블록체인은 **분산원장 기술(DLT: Distributed Ledger Technology)**이라고도 불리며, 이는 거래 정보를 기록한 원장 데이터를 중앙 서버가 아닌 참가자들이 **공동으로 기록 및 관리**하는 것을 의미한다.
- 블록체인은 **분산처리와 암호화** 기술을 동시에 적용하여 높은 **보안성**을 확보하는 한편 거래 과정의 신속성과 투명성을 특징으로 한다. 보안성의 강화로 해커의 공격과 데이터의 왜곡 그리고 기존 중앙집중 서버 방식(Central Server)에서 가장 큰 문제인 디도스 공격을 원천적으로 방어할 수 있다.

블록체인 network

블록체인(BLOCKCHAIN)이란?

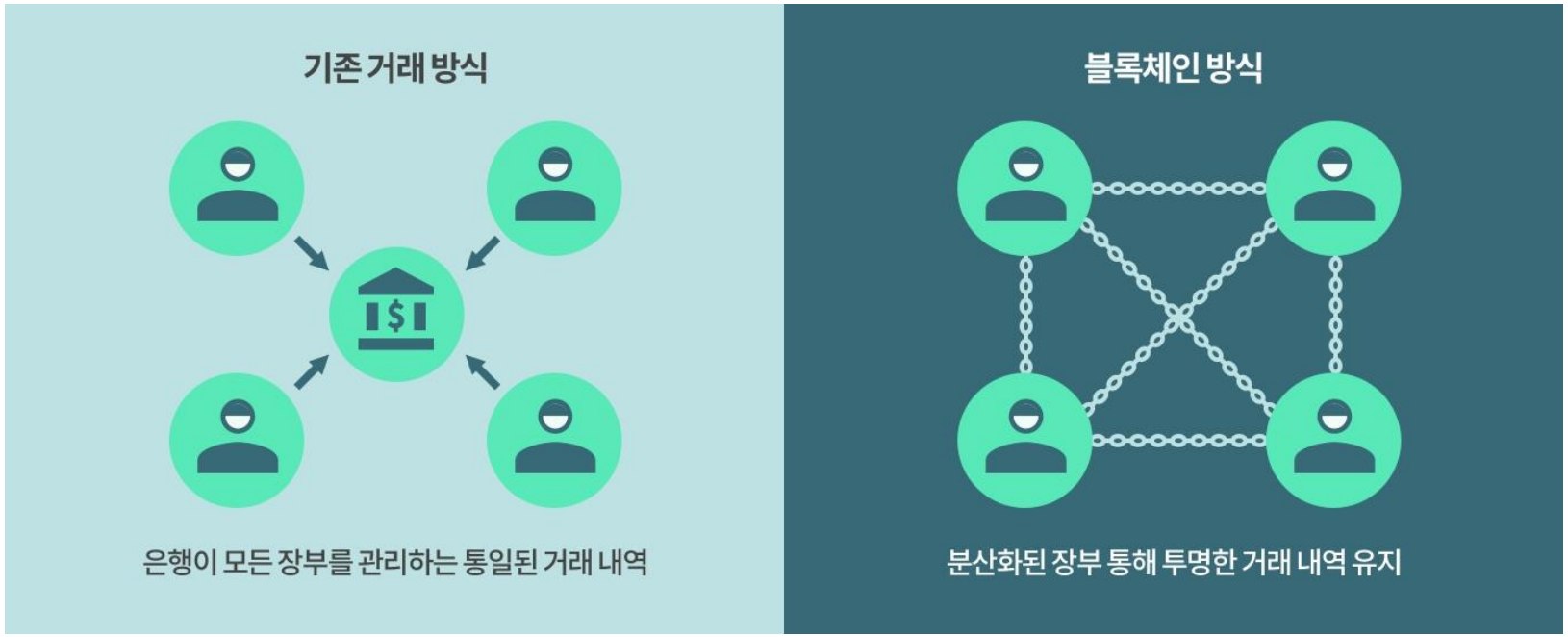




P2P-network

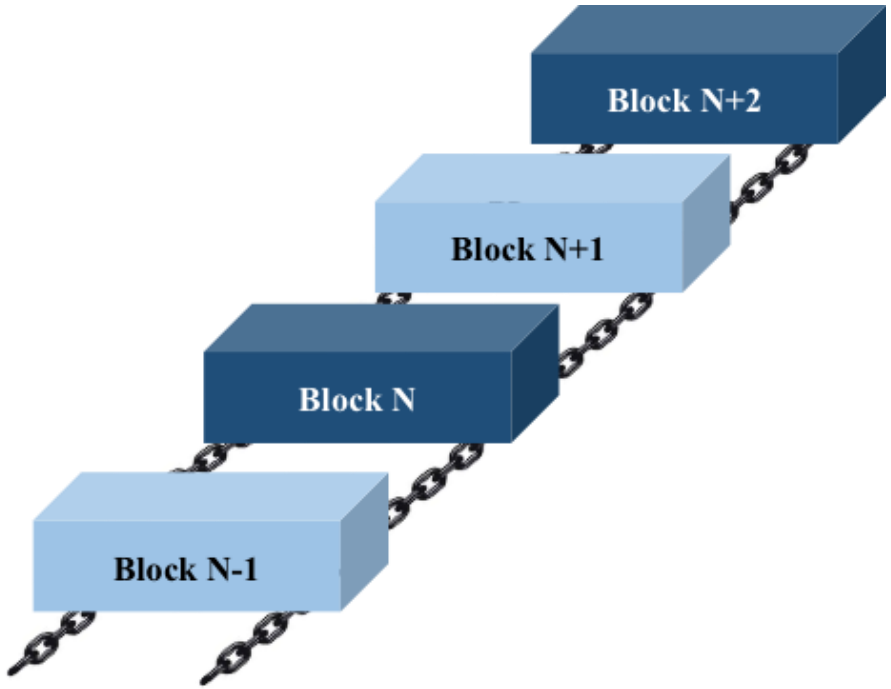
블록체인(BLOCKCHAIN)이란?

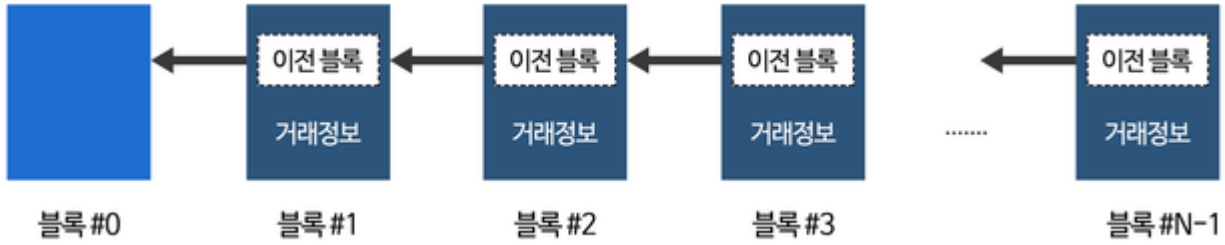
- 분산되어 저장 한다는 것은 **탈중앙화**를 의미 한다. 즉 중앙의 간섭없이 모든 원장을 관리하는 것이 블록체인의 **분산원장관리**인 것이다.



블록체인(BLOCKCHAIN)이란?

- 블록들을 **체인 형태**로 묶은 형태이기 때문에 블록체인이라는 이름이 붙었다. 블록들이 형성된 후 시간의 흐름에 따라 순차적으로 연결된 **'사슬(체인)'**의 구조를 가지게 된다.



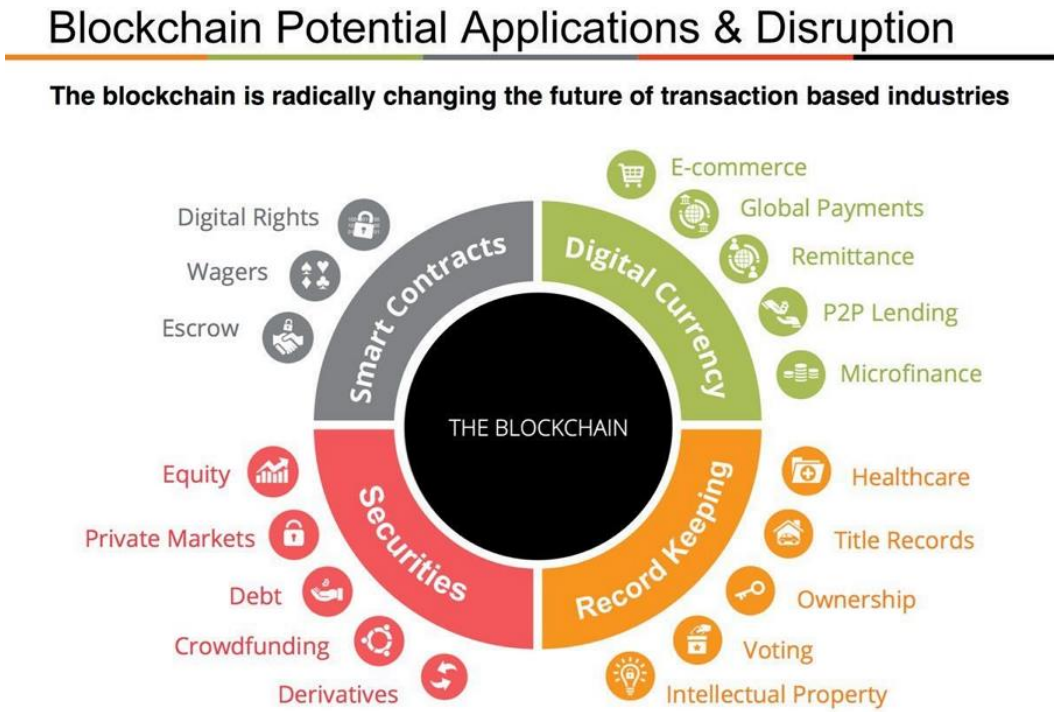


블록체인의 특장점

- 블록체인은 **분산저장** 을 한다는 점이 특징이다. 기존 거래방식에서는 **데이터를 위,변조** 하기 위해선 **중앙 서버**를 공격하면 됐다. 그러나 블록체인의 경우 여러 명이 **동일한 데이터**를 저장하기 때문에 위, 변조가 어렵다. 블록체인 네트워크를 위, 변조하기 위해서는 **참여자(노드)**의 거래 데이터를 모두 공격해야 하기 때문에 사실상 해킹이 불가능하다.
- 블록체인은 **중앙 관리자**가 필요 없다. 중앙기관이나 관리자 없어도 다수가 **데이터를 저장, 증명**할 수 있기 때문에 **탈중앙** 이 가하다.

블록체인의 기술 활용

- **금융거래**에서는 이미 블록체인 기술을 도입하고 있다. 점진적으로 **개인 의료 정보** 뿐 아니라, 다른 산업으로 확대하기 위한 검토 단계에 있다. 특히 네트워크를 통한 콘텐츠 서비스 요소, 즉 **영상 또는 이미지, 음원과 같은 콘텐츠**에도 가치를 부여하고 이를 **개별적**으로 거래하기 위한 수단으로 활용하는 시도가 시작되었다.
- 그 외에도 **전자 계약 시스템**에도 검토되고 있다. 계약서(또는 문서)를 블록체인으로 접목하여 **위/변조**가 불가능하게 하고, **계약 체결의 조건**이 만족되었을 때 **원본이나 증명이 가능한 문서**로써 보장하는 기술로도 적용할 수 있다.
- **부동산 시장** : 블록체인은 **소유권 증서의 등록, 추적 및 양도**에 보다 효율적인 생태계를 조성하는 방법을 제공한다. 또한 당사자들이 관련 문서의 유효성을 검증할 수 있는 방법을 제공한다.
- **의료 부문** : 블록체인은 암호화된 데이터베이스를 통해 사용자에게 **의료 정보**를 제공할 수 있다. 병원 정보를 **분산화** 된 의료 데이터베이스와 연결하고, 기록을 안전하게 **공유**할 수 있게 된 것이다.
- **인적 자원** : 블록체인에 저장되어 있는 정보를 바탕으로 채용자는 **학업 기록** 등에 접속하여 주어진 정보 및 배경의 유효성을 검증할 수 있다. 이 기술은 학위 조작의 위험을 줄이는 동시에, **발급 및 보관에 드는 비용**을 줄일 수 있다는 장점을 가진다.

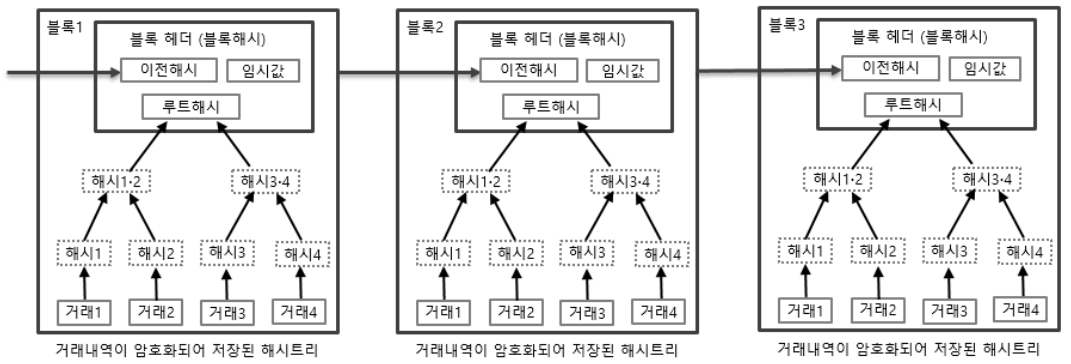


블록체인의 기술동향

- 시장조사기관 가트너에 따르면 2020년에는 사업적 부가가치의 **연간성장률이 120%**에 이르고, 2030년에는 사업적 부가가치가 약 **3조 달러**를 초과할 것으로 예측되고 있다. 블록체인 기술은 신뢰성 및 안정성을 바탕으로 현재 금융, 유통, 물류, 제조, 공공 서비스 등 다양한 분야에 적용되고 있으며, 데이터의 보안성 및 신뢰성이 보증되어야 하는 보험, 가상화폐, 개인인증, 유통 등의 분야를 중심으로 블록체인 활용이 확대되고 있는 상황이다.
- 블록체인의 중요한 특징은 ***해쉬(Hash)** 함수를 사용한다는 것이다. 해쉬 함수를 사용하는 이유는 입력 데이터에 대해 **변경할 수 없는 결과 값**을 출력함으로써 데이터의 **오류나 변조를 방지**할 수 있는 완전 무결성을 제공할 수 있기 때문이다.
- 블록체인은 또한 해시 캐시 기술을 활용해 **작업 증명**을 할 뿐만 아니라, 블록과 블록을 해쉬로 **연결**하고 블록체인의 **신뢰**가 강화되도록 네트워크 참여자의 경쟁적 검증을 유도할 수 있어서 데이터를 안전하게 거래하는 **플랫폼** 역할을 수행할 수 있다. 따라서 **전자서명**과 같이 사용되는 경우에는 더욱 효율적인 서명 생성을 가능하게 할 수 있으며, 사실상 **데이터 조작이 불가능**하기에 보안 분야에 적극 활용되고 있다.
- 최근 아마존, 구글, 애플과 같은 거대 인터넷 기업들은 4차 산업혁명의 핵심 ICT 기술인 클라우드 컴퓨터를 이용하여 P2P 생산의 결과물을 자신들의 데이터센터에 저장하는 구상을 하고 있는데, 이는 데이터의 축적, 관리 접근, 이용 등을 본인들의 통제 하에 두려는 의도로 해석되고 있다.
- 블록체인의 **투명성, 비가역성, 신뢰성**은 이용료의 **정산, 배분**에 있어서의 고질적인 문제에 대한 해결책으로 사전에 정해진 바에 따라 집행이 보장되는 ***스마트 계약**을 활용하여 이용료 징수와 배분의 불이행에 따른 다툼을 원칙적으로 방지할 수 있다.
- * **해쉬 함수**? – **불 특정한 길이의 데이터를 입력하면 고정 된 길이의 암호화된 값을 출력**하는 함수이며, 이 해시 함수에 의해 얻어지는 값을 해시라고 정의.
- ***스마트 계약**? - 1994년 암호학자이자 프로그래머인 닉 자보(Nick Szabo)가 스마트 계약이란 개념을 처음 선보였으며, 닉 자보는 스마트 계약을 **"계약에 필요한 요소를 코드를 통해 스스로 실행되게 하는 전산화 된 거래 약속"**이라 정의하였음.

블록체인(BLOCKCHAIN) 동작 원리

- 하나의 새로운 블록을 구성한 경우, 마치 **체인처럼** 이전부터 이어져 내려오던 블록체인의 **맨 끝에 이 새로운 블록을 연결**시켜야 한다. 새로운 블록을 기존 블록체인의 끝에 연결시키려면, 해당 블록의 이름에 해당하는 해시 값을 찾아내야 한다. 새로운 해시 값을 성공적으로 찾아내는 경우 새로운 블록이 생성되어 기존 블록체인에 연결된다.
- 새로 구성한 블록의 이름에 해당하는 해시를 찾아내는 일은 **수없이 많은 시도를 반복**해야 하는 매우 힘든 과정이다. 왜냐하면 새로운 블록의 해시는 반드시 프로그램에 의해 미리 정해진 **목표 값보다 작아야 한다는 조건을 충족**해야 하기 때문이다. 예를 들어, **목표 해시 값이 00ff32**라고 가정하고, 새로 만든 블록의 해시 값이 **12fa3b**라고 하면, 이 값이 목표 값 보다 더 크기 때문에 블록 생성에 실패하게 된다. 하지만 새로 찾아낸 해시 값이 00c3b1이라고 가정하면, 이 값은 목표 값보다 더 작기 때문에 새로운 블록의 생성에 성공하게 된다.



블록체인 합의 알고리즘

PoW(Prooof of Work) - 작업증명

- **PoW**는 **작업증명** 이라고 한다. 문제(**특정 조건을 만족하는 해시 값 찾기 특정 길이 특정 해시 값 이하의 해시 값 찾기**)를 주어 주고 조건을 만족하는 답을 찾아낸 노드에게 보상하는 합의 알고리즘입니다. '**사토시 나카모토'(Satoshi Nakamoto)**가 제안한 최초의 블록체인인 비트코인을 통해 제안된 합의 알고리즘이다.
- 동작 방식을 조금 더 들여다 보면 해시 값에 대한 조건이 주어지고 노드들은 해시 값을 구하기 위해 컴퓨팅파워를 동원해 값을 찾고 값을 찾으면 새로운 블록을 추가하여 **브랜치**를 형성한다.브랜치가 생겼을 때 가장 긴 블록체인이 남은 브랜치가 최종 브랜치로 결정되며 나머지 브랜치는 버려지게 되며 과반수이상의 노드가 합의한 거래가 원본으로 채택되게 된다.
- **장점**: **답을 찾아낸 노드가 이익을 가져가는 구조**로 되어있고 모든 노드들이 서로 부정행위가 방지되도록 경계하는 구조로 탈중앙화가 가능하다. 최초의 제안된 비트코인의 합의 알고리즘으로 해시함수를 통해서 블록체인을 형성하고 임의로 조작하기 힘든 강력한 보안성을 갖고 있다.
- **단점**: 하지만 조건을 만족하는 답(**해시 값**)을 찾기 위해 막대한 **컴퓨팅파워**가 필요해 많은 전력, **에너지가 낭비**되고 트랜잭션이 완료되기까지 **많은 시간**이 걸리고 느리다는 단점이 있다. 비트코인의 예를 들면 **특정세력 또는 집단**이 컴퓨팅 파워로 **해시를 독점**하여 생태계가 **교란**될 가능성이 있다. 중국에 기반을 둔 마이너들이 컴퓨팅 파워를 점유하면서 독점 및 네트워크의 통제 우려가 커지고 있다.
- **관련블록체인**: **비트코인, 이더리움, IOTA, 라이트코인, 비트코인캐시, 비트코인골드, 모네로**

블록체인 합의 알고리즘

PoS(Proof of Stake) - 지분증명

- PoS는 해당 블록체인에 대해 가지고 있는 **지분 율로 보상** 받게 되는 합의 방식이다. 즉 지분을 많이 가진 노드에 **블록을 생성**할 수 있는 **권한**을 부여하는 것이다. 많은 지분을 가지고 있을수록 보상을 받게 되고 **해당 노드**는 그 가치를 유지하기 위해 **전체 네트워크를 배반하지 않고** 유지할 것이라는 개념이다. **이자와 같은 방식으로 보상**이 지급되고 코인을 보관하고 있는 지갑을 **네트워크에 연결**시키면 보상을 받을 수 있다.
- PoS는 여러 시나리오(독점, 과점, 비이성,공격 등)에서 안정적인 블록체인으로 수렴한다는 것이 게임이론으로 증명되었다.
- 이더리움 2.0부터는 PoW에서 PoS로 합의 알고리즘을 변경하려고 하고 있다.

- **장점:** 가장 큰 장점은 해시를 찾기 위한 컴퓨팅 파워가 필요하지 않아 경제적이고 친환경 적이라고 할수 있습니다. 일반인이던 전문 miner(채굴자)이던 효율이 같기 때문에 자연스레 분산되고 탈중앙화가 가능하다.
- **단점:** 반면 검증이 되지 않아 보안성에 대한 risk와 우려가 있습니다. 지분을 많이 가진 노드들이 **독점**할 수 있는 가능성도 배제할 수 없다.
- **관련블록체인: NEO, ADA, 스트라티스**

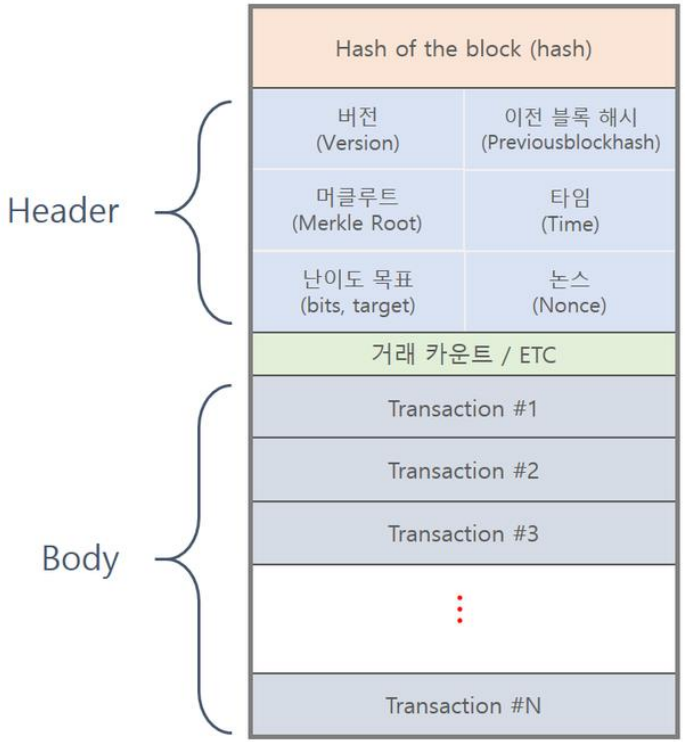
블록체인 합의 알고리즘

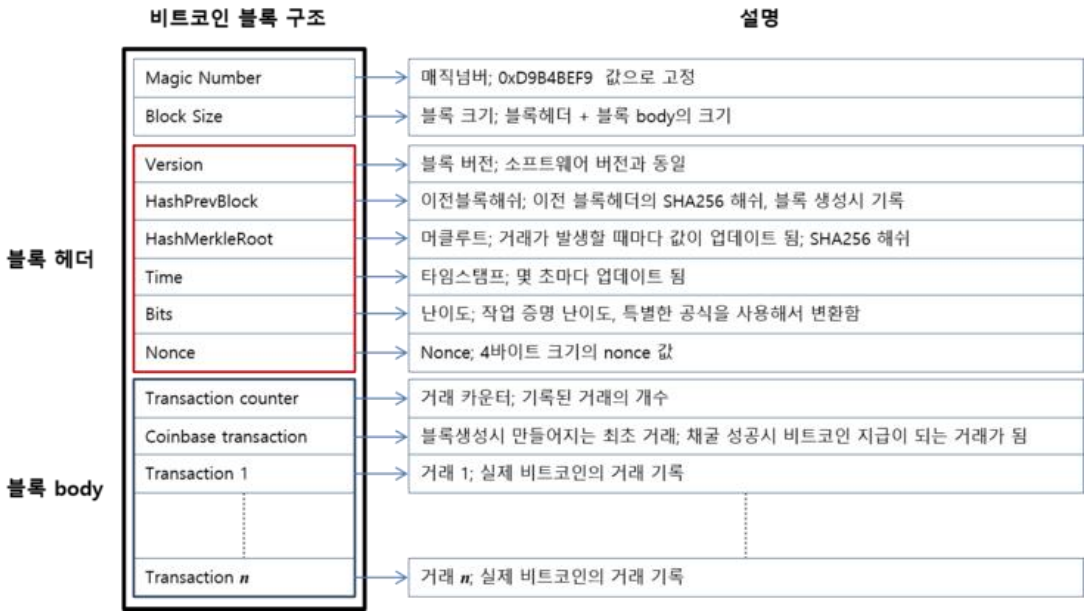
DPoS(Delegated Proof of Stake) - 위임지분증명

- **DPoS**는 **위임지분증명** 이라 부르기도 하며 말그대로 위임된 POS이다. PoS가 자산을 가진 사람들이 전부 참여할 수 있는 방식이라면 **DPoS는 특정 인원에게만 POS를 할 수 있도록 권한을 위임하는 것이다.** 즉 특정인 몇 명만이 블록을 생성하여 증명할 수 있습니다.
- **DPoS** 네트워크는 구성하는 모든 노드들의 투표 결과로 정한 상위 노드에게 권한을 위임하여 일종의 대표자가 되는 것이다. PoS의 경우, 일정 지분을 소유한 모든 노드에게 블록 생성 권한이 주어지기에 오랜 시간이 필요하지만 DPoS의 경우, 투표 결과로 정한 상위 노드 라는 비교적 적은 숫자로 인해 합의 시간과 비용을 줄일 수 있다. 합의 시간과 비용이 줄어든다는 것은 **전송처리가 굉장히 빠르다**는 것과 밀접한 관련이 있습니다.
- **DPoS는 PoS와 달리 소규모 참여자에게는 꿀단지 이다.** PoS는 참여하기 위해 최소 코인을 (말이 최소지 어마어마한 돈) 가지고 있고 **블록생성을 위해 24시간 네트워크를 유지**하며 하드포크마다 알고리즘 업데이트를 할 필요가 없다. **소규모 참여자는 권한을 위임하고 위임한 상위노드로부터 이자를 받거나 송금 수수료를 감면 받을 수 있다.**
- 상위 노드로서 뽑힌 사용자는 **PoS에서와 같이 블록생성**을 진행할 수 있다. 상위 노드로 뽑히는 기준은 **본인을 투표한 구성원의 코인 총 합 순위**로 매기는 것이 보통의 방법이다.

- **장점:** 합의에 참여하는 노드가 한정되기 때문에 매우 빠른 속도(건당 0.5초)와 확장성을 가집니다. PoS와 마찬가지로 **블록생성 비용**이 아주 낮다.
- **단점:** 권한을 위임 받은 노드들이 **담합**을 할 위험성이 있다. 또한 공개된 소수의 노드들에 대한 **보안 공격(DDoS등) 위험**도 존재한다. 블록생성에 대한 권한을 위임하기 때문에 탈중앙화 되지 않았다는 비판이 있을 수 있다.
- **관련블록체인: 스팀, 이오스, 아크, 라이즈**

블록의 구성요소

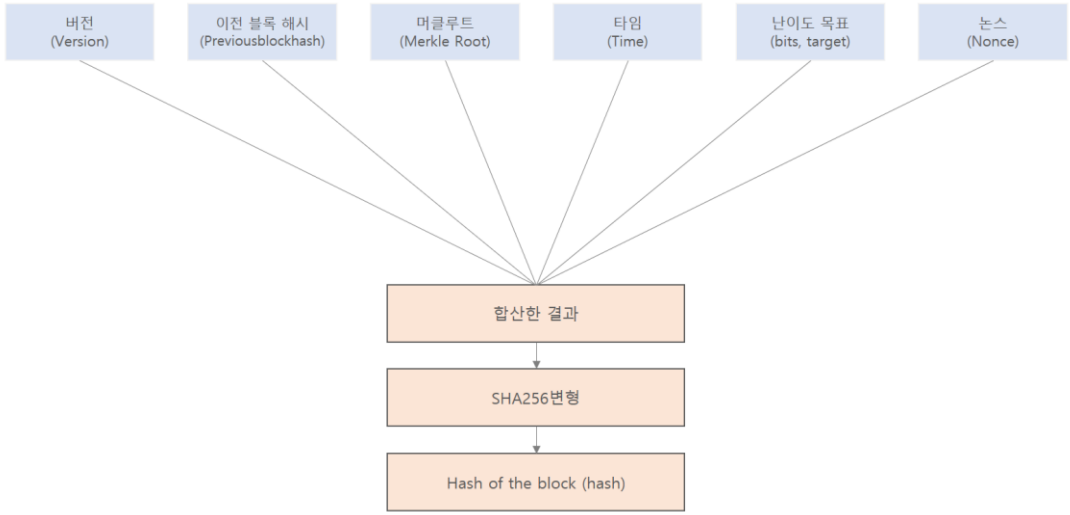

Hash of the block (hash)
버전
(Version)
이전 블록 해시
(Previousblockhash)
머클루트
(Merkle Root)
타임
(Time)
난이도 목표
(bits, target)
논스
(Nonce)
Header
거래 카운트 / ETC
Transaction #1
Transaction #2
Transaction #3
Transaction #N
Body


비트코인 블록 구조
설명
Magic Number
매직넘버; 0xD9B4BEF9 값으로 고정
Block Size
블록 크기; 블록헤더 + 블록 body의 크기
블록 헤더
Version
블록 버전; 소프트웨어 버전과 동일
HashPrevBlock
이전블록해쉬; 이전 블록헤더의 SHA256 해쉬, 블록 생성시 기록
HashMerkleRoot
머클루트; 거래가 발생할 때마다 값이 업데이트 됨; SHA256 해쉬
Time
타임스탬프; 몇 초마다 업데이트 됨
Bits
난이도; 작업 증명 난이도, 특별한 공식을 사용해서 변환함
Nonce
Nonce; 4바이트 크기의 nonce 값
블록 body
Transaction counter
거래 카운터; 기록된 거래의 개수
Coinbase transaction
블록생성시 만들어지는 최초 거래; 채굴 성공시 비트코인 지급이 되는 거래가 됨
Transaction 1
거래 1; 실제 비트코인의 거래 기록
Transaction n
거래 n; 실제 비트코인의 거래 기록

블록의 구성요소

블록 해시(Hash of the block)

- **블록 해시**는 쉽게 **'블록'의 이름 정보**라고 생각하면 될 것 같다. 블록 해시는 블록의 헤더 정보인 **버전**, **이전 블록 해시**, **머클 루트**, **타임**, **bits**, **논스** 정보를 모두 더하여 **합을 구한 후 SHA256으로 변환한 결과 값**이다.
- 그림처럼 블록 헤더 정보(버전 + 이전 블록 해시+ 머클 루트 + 타임 + bits + nonce)의 합산 정보를 구한 후 SHA256으로 변환하면 블록의 블록 해시 값을 구할 수 있다. (**여기서 합산한다는 의미 그리고 단순히 SHA256으로 변환해서는 정확한 블록 해시 값을 구할 수 없다.**)
- **우선 개념적으로는 헤더 정보를 모두 합산하여 SHA256 변환하면 블록 해시 값을 추출할 수 있다고만 이해할 것.**



블록의 구성요소

버전

- **해당 블록의 버전**이다.
- 현재 이 블록 헤더를 만든 **코인 프로그램의 버전 정보**이다.

블록의 구성요소

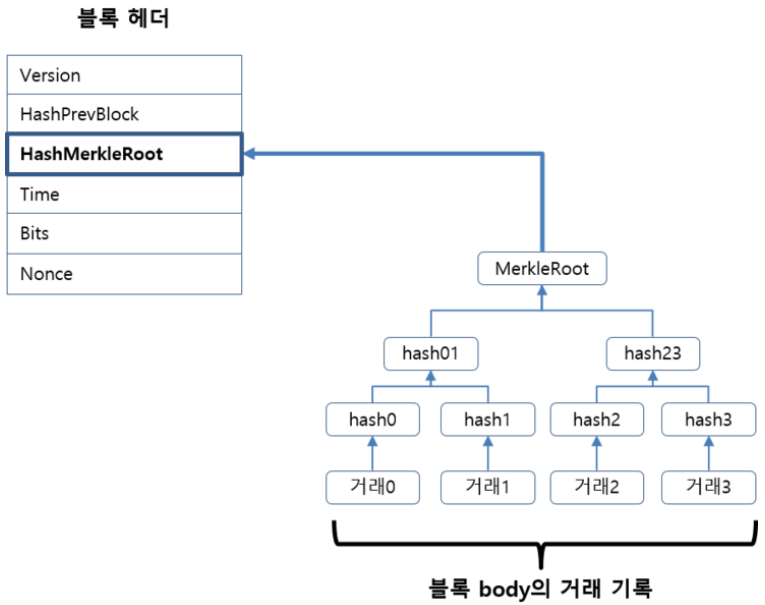
이전 블록 해시(Previousblockhash)

- 앞서 블록체인은 거래 정보의 묶음인 블록이 체인 형태로 연결되어 있다고 설명했다. 이름에서도 직관적으로 알 수 있듯이 이전 블록 해시 정보는 **이전 블록의 주소 값을 가리키는 요소**이다.
- 그림처럼 각 블록의 헤더 정보에는 **이전 블록의 해시정보**를 가지고 있다. 각 블록이 이전 블록의 해시 정보를 가지고 있기 때문에 각 블록이 서로 서로 연결되어 있는 구조가 될 수 있다.

블록의 구성요소

머클 루트(Merkle Root)

- **'머클 루트'는 블록의 바디 부분에 저장된 트랜잭션(거래 정보) 들의 해시 트리이다.** 각 트랜잭션과 가까운 노드 끼리 쌍을 지어 해시 값을 구하여 최종적으로 구해진 해시 값이 머클 루트 해시 값이다.
- **머클 루트의 역할**
  1. '머클 루트'(머클 해시)값을 통해 단일 블록 내에 존재하는 **트랜잭션의 무결성을 검증**할 수 있다.
  2. '머클 루트'(머클 해시)값을 이용하여 블록의 해시 값을 생성하였기 때문에 **블록의 해시의 무결성도 함께 검증**할 수 있다.
- **해당 블록이 유효한지에 대한 무결성을 검증**하기 위한 요소가 머클 루트 혹은 머클 해시라는 구성요소이다.



블록의 구성요소

타임(Time)

- 해당 블록의 **대략적인 생성 시간을 의미** 한다.
- 타임 스탬프는 **유닉스** 기준일 자로 표시되며 **1970년 1월 1일 자정부터 경과한 시간을 초 단위**로 계산한 값이다.
  1. 예제 사이트: https://www.unixtimestamp.com/

블록의 구성요소

bits

- bits는 **난이도 해시 목표 값을 의미하는 지표이다.**

난이도 설정값인 4바이트 Bits를 target으로 변환하는 공식

Bits = 0x1b0404cb 인 경우,
Bits의 앞 2자리와 뒤 6자리를 아래와 같이 분리함

1b 0404cb

작업 증명 대상 target의 값은 다음과 같이 구함

→ **target = 0x0404cb * 2**(8*(0x1b-3))**

블록의 구성요소

Nonce

- nonce는 **블록을 만드는 과정에서 해시 값을 구할 때 필요한** 재료 역할을 수행한다.
- 비트코인에서 작업 증명은 이 **target보다 작게 나오는 블록 헤더**의 해쉬 값이 되도록 Nonce를 구하는 것입니다. 그런데, SHA256 해쉬는 32바이트, 16진수로 64자리로 표현됩니다.
- 위 예의 target을 64자리 16진수로 표현하면 다음과 같다.
  - **target = 0x00000000000404cb000000000000000000000000000000000000000000000000**
- 이 **target 값이 작업 증명의 대상이 되는 값**이며 비트코인의 블록 헤더의 **SHA256 해쉬 값이 이 값보다 작거나 같은 해쉬 값이 나오는 Nonce**를 구하게 되면 **채굴 성공**인 것이다.

BITCOIN

개요

- **We define an electronic coin as a chain of digital signatures**. Each owner transfers the coin to the next by digitally signing a hash of the previous transaction and the public key of the next owner and adding these to the end of the coin. A payee can verify the signatures to verify the chain of ownership.
- **우리는 전자 화폐를 디지털 서명의 체인으로 정의합니다**. 코인 소유자는 이전 거래 내역과 다음 소유자의 공개 키와의 해쉬 값을 코인 맨 뒤에 붙입니다. 돈을 받은 사람은 앞 사람이 유효한 소유자였다는 것을 확인할 수 있습니다.

BITCOIN

Bitcoin 이란?

- 비트코인은 **사토시 나카모토**에 의해 2008년 10월에 "Bitcoin: A Peer-to-Peer Electronic Cash System"이라는 제목의 9쪽짜리 논문을 통해 https://bitcoin.org/bitcoin.pdf 공개되었다. 2009년 1월 3일에 비트코인이 처음 발행**(제네시스블록)**되었으며 2009년 2월 11일에 Bitcoin Core v0.1 프로그램이 공개되었다. 그리고 공개를 하면서 사토시 나카모토는 **"재래 통화의 뿌리 문제는 그것이 작동하게 하는데 필요한 모든 신뢰입니다. 중앙은행은 통화 가치를 떨어뜨리지 않도록 신뢰할 수 있어야 하지만, 화폐 통화의 역사는 그 신뢰의 위반으로 가득합니다."**면서 기존 금융에 대한 비판을 했다.(제네시스블록의 트렌젝션에 메세지 **"The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"**을 남겨뒀으며 2009년 1월 3일 런던 뉴욕타임즈 1면의 "더 타임스, 은행들의 두 번째 구제금융을 앞두고 있는 U.K. 재무장관" 기사다.)
- 비공식 코드는 **'XBT'** 또는 **'BTC'**이며, 한국에서는 세간에서 **'빗코'** , **'비트'** , **'머장(대장)'** 으로 줄여 부르기도 한다. 비트코인 등의 암호화폐는 법정 통화가 아니므로, ISO 등에서 표준화한 코드는 아니다. 가장 많이 쓰이는 3글자 약칭인 **'BTC'**는 단순히 **'BiTCoin'**의 약자일 뿐이며, 'XBT'는 ISO 4217 스타일의 작명법을 유용한 것이나 역시 공식적인 코드가 아니다.
- 이 문서를 포함한 대부분의 거래소에서는 비트코인 개발자가 주도하는 **'Bitcoin Core'** 클라이언트를 구동하는 블록체인만 **'비트코인'**이라고 칭하고 있다.
- 기존 화폐와 달리 정부나 중앙은행, 금융기관의 개입 없이 **개인간(P2P)**의 빠르고 안전한 거래가 가능하며, 정부가 원하면 더 찍어낼 수 있는 기성 화폐와는 달리 최대 **발행량이 한정**되어 있다는 것이 특징이다.

BITCOIN

Bitcoin 이란?

- 향후 100년간 발행될 화폐량이 미리 정해져 있고, **2100만 개까지** 발행 된다. 현재는 약 1500만 개 정도가 발행되었으며(**2015.2.4기준**), 앞으로 600만 개가 더 발행될 예정이다. 세계 통화로 사용되기는 턱없이 부족한 숫자지만 1BTC가 소숫점 아래 8자리, 즉 10^{-8} BTC = 0.00000001BTC까지 분할이 가능하다.
- 앞으로 발행될 모든 비트코인의 총량이 2100만 개이니, 결과적으로는 현재 기준으로 21,000,000 * 100,000,000 = 2,100,000,000,000,000(2100조) 사토시가 유통될 수 있다.

BITCOIN

특징

- 최근에 만들어지는 **블록체인 기반 코인**들과는 다르게 **결제나 거래 관련 시스템 즉 화폐로서의 기능에 집중**되어 있다. 예를 들어 **이더리움**은 다양한 어플리케이션으로 발전 될 수 있는 **플랫폼** 적 기능을 하는데 그에 따라 **베이직 어텐션 토큰(BAT), 골렘(GOLEM), 어거(AUGUR), 노시스(Gnosis)** 등 많은 코인이 만들어지는 데 기초 플랫폼을 제공하였다.
- 비트코인은 **가장 처음에 만들어진 암호화폐**이기에 그런 것도 있고, 한 가지 기능에만 집중되어 있는 것이 나쁜 것은 아니다. 그러나, 점차 점점 전송속도에 문제가 생겨 화폐 기능도 온전하게 이루어지지 못함에 따라 **비트코인 캐시, 라이트코인, 비트제니** 등 수많은 아류작이 나타나게 된다. 비트코인 캐시의 탄생은 채굴자들간의 이권 다툼이 더 크게 작용하긴 했다.

BITCOIN

Mining(채굴)

- 비트코인은 **비잔틴 장군의 문제**를 블록 체인과 작업 증명으로 해결했다. 배신자가 50%를 초과하면 문제가 되지만 지금은 네트워크가 워낙 커져서 가짜 화폐가 나올 수 없을 정도의 네트워크를 구축한 상태이기 때문에 안심하고 사용해도 된다.
- 비트코인을 생성하는 것은 금광 채굴에 빗대어 **"채굴"** 이라고 불리기도 한다. 사용자가 코인 묶음을 받을 수 있는 확률은 정해진 목표 값 이하의 해시를 만들어낼 수 있는 확률과 같으며, 비트코인이 묶음 당 생성되는 양은 50 BTC를 넘지 않는다. 그리고 변동 분은 21만째 블록이 될 때 마다 1/2으로 줄어들게 프로그램되어 전부 2100만을 넘지 않게 된다. 이 지불 금이 줄어들면, 사용자들은 **블록을 생성하는 노드를 구동하는 것보다는 거래 수수료를 벌도록 유도**된다.

BITCOIN

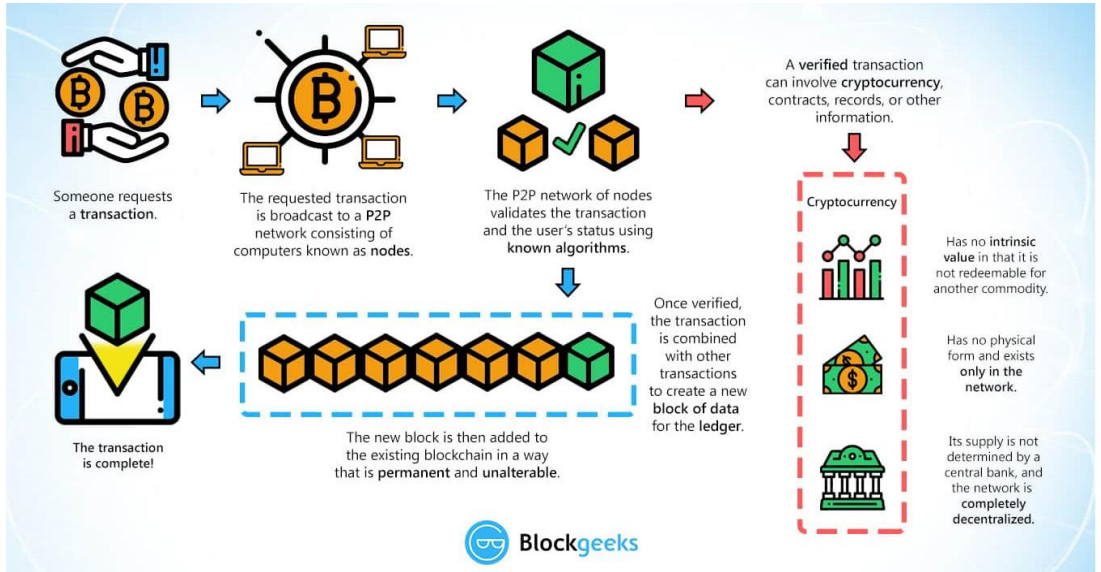
Mining(채굴)

- 네트워크의 **생성용 노드**들은 전부 그들의 후보 **블록을 만들기 위한 암호화** 문제를 찾아내기 위해 경쟁한다. 이 문제를 풀려면 반복적인 시행착오가 필요하다. 노드가 **정답을 찾으면** 네트워크의 나머지 노드에게 그것을 알리고 **새로운 비트코인 묶음**을 요구한다. 새로 해결된 블록(solved-block)을 받은 노드들은 그것을 허가하기 전에 **인증하고 체인**에 추가한다. 노드에는 **표준 클라이언트**를 사용하거나 **GPU 가속을 이용하는 다른 소프트웨어**가 사용될 수 있다. 사용자들은 집단으로 비트코인을 생성할 수도 있다.
- 일반적인 인식과는 달리, **2017년**에는 비트코인 채굴에는 **그래픽카드**가 거의 사용되지 않고 있다. 그러나 그후에 CUDA 라이브러리를 이용한 **GPU Mining**이 많이 이용 되었다. 비트코인 채굴(Mining)은 기존 화폐의 **중앙은행**처럼 통화의 공급과 거래의 보증을 책임지는 역할을 한다. 그러나 중앙은행과 달리 채굴은 네트워크를 통해 **P2P 방식**으로 진행된다.
- 이 과정에서 **가장 먼저** 블럭 생성에 성공하는 노드에게만 **현상금**이 주어지므로, 각 채굴 노드는 현상금을 먼저 받기 위해 경쟁하게 되고, 동시에 다른 채굴 노드가 **잘못된 거래**가 담긴 블럭을 생성할 경우 자신의 이득을 위해 거절하게 된다.

블록체인 기술

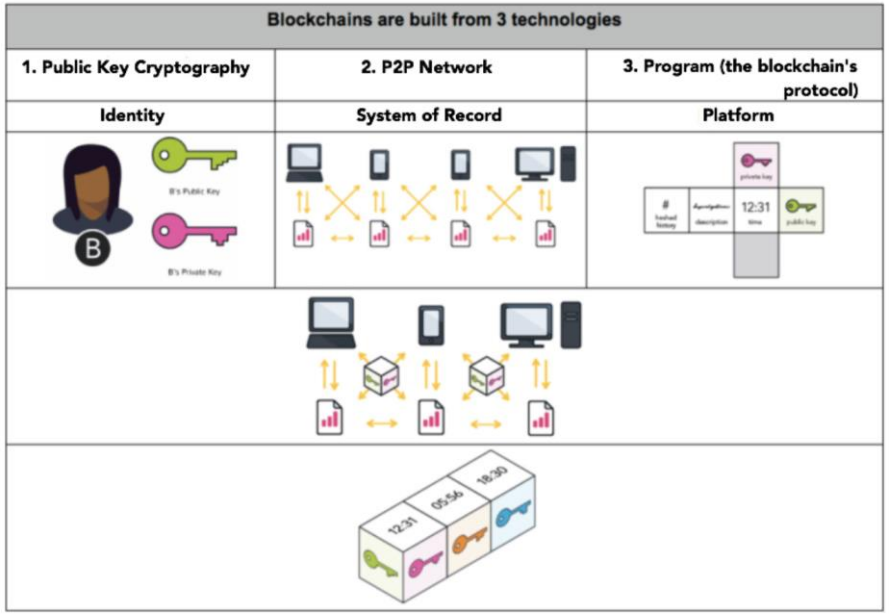
기본 동작 원리

- 블록체인은 **거래 발생 시 블록(Block)을 생성**하며, 기록을 계속 보관하기 위해 기존 블록에 **체인(Chain)처럼** 연결한다. 신규 블록들은 **이전 거래 내역 데이터와 연계**하여 블록을 생성하기 때문에, 블록이 계속 생성될수록 안정성이 강화되는 구조를 갖는다는 특징 이 있다. 블록체인은 같이 **투명하고 안전한 방식**으로 **거래 당사자 간 정보를 전달**하는 간단하면서도 **독창적인 방법**으로, 거래 당사자는 **블록을 생성하여 프로세스를 시작**한다. 이 블록은 수천 개, 아마도 수백만 대의 컴퓨터가 인터넷에 분산되어 있는지 확인하며, **검증된 블록은 체인에 추가**된다. 이후, 체인 전체에 저장되어 고유한 레코드뿐만 아니라 고유한 기록을 가진 고유한 레코드를 생성하고 **공개(분산)원장**에 기록하게 된다. 이때 단일 레코드를 **위조**하는 것은 **수백만의 인스턴스에서 관련된 전체 체인을 변조**하는 것을 의미하며, 이는 사실상 불가능하여 보안 성이 뛰어나다고 볼 수 있다. 이와 같이 거래를 투명하고, 안전하게 보호하기 위한 블록체인의 구성요소 기술로 **공개키 암호화, P2P 네트 워크, 블록체인 프로토콜** 등이 있다.



블록체인 기술

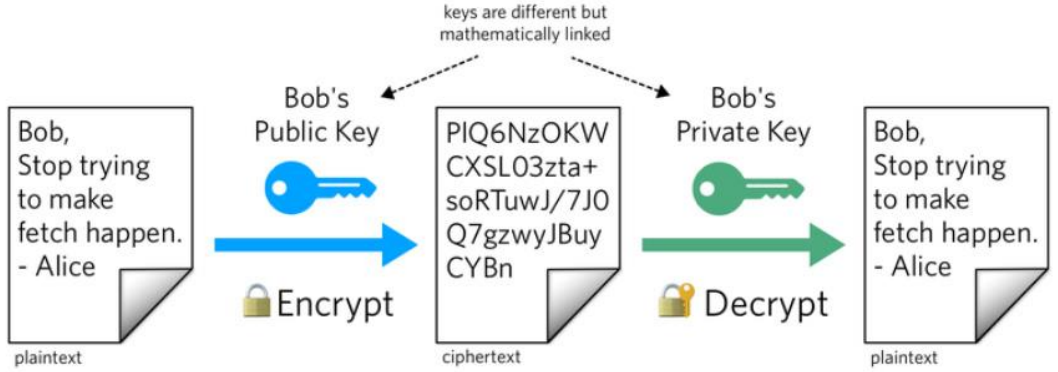
블록체인의 3대 핵심기술



블록체인 기술

공개키 암호화

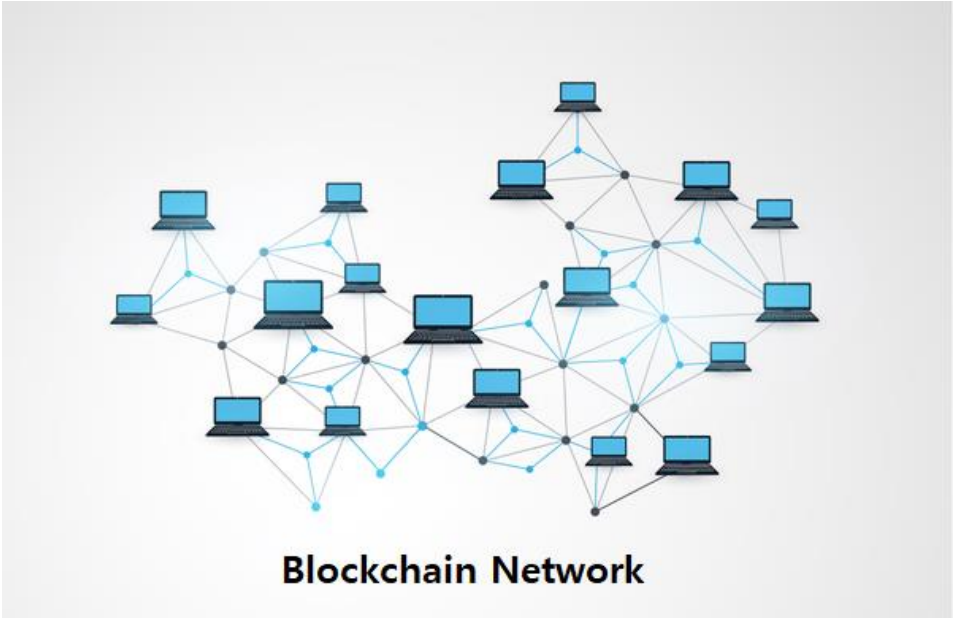
- 공개키 암호화는 **공개키(Public key)**와 **개인키(Private key)** 쌍을 사용하여 다른 작업을 수행하며, 공개키는 **널리 배포**되고 개인키는 **비밀로 유지**된다.
- 개인의 공개키를 사용하면 **개인키를 가진 사람만 암호를 해독**하고 읽을 수 있도록 메시지를 암호화할 수 있다.
- 개인키를 사용하면 해당 공개키를 가진 사람은 누구나 개인키 **소유자가 메시 지를 작성**하고 그 이후로 수정되지 않았음을 확인할 수 있도록 **디지털 서명을 작성**할 수 있기 때문에 블록체인은 공개키 암호화를 광범위하게 사용할 수 있다.



블록체인 기술

P2P 네트워크

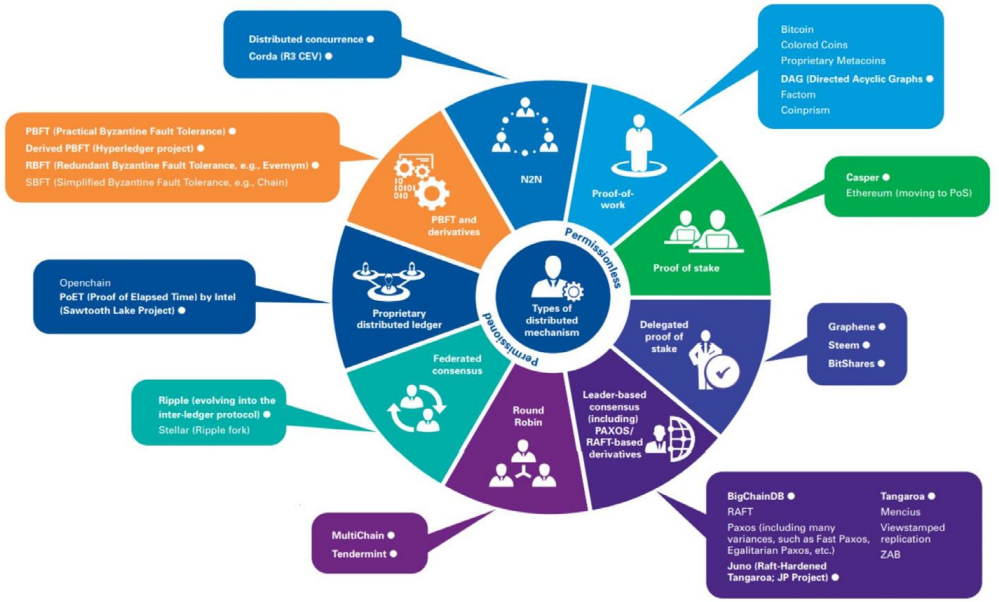
- P2P(Peer-to-Peer)는 **집합적으로 파일을 저장하고 공유**하는 장치 그룹으로 구성된다.
- 네트워크에 참여하는 **노드**는 블록체인 정보를 가지고 있으며, **동일한 거래 내역이 분산저장**되어 관리되며, 거래가 이상 없음을 확인하는 **분산 합의 제도**를 채택하고 있으며, 별도의 추가적인 신용 기관 없이 P2P에서 검증한다.
- 블록체인 기술에 내재된 P2P 아키텍처는 **비트코인 및 기타 암호화폐를 중개자나 중앙 서버 없이** 전세계로 전송할 수 있게 한다. 또한, 블록을 확인하고 검증하는 프로세스에 참여하려는 경우 누구나 노드를 설정할 수 있게 한다.



블록체인 기술

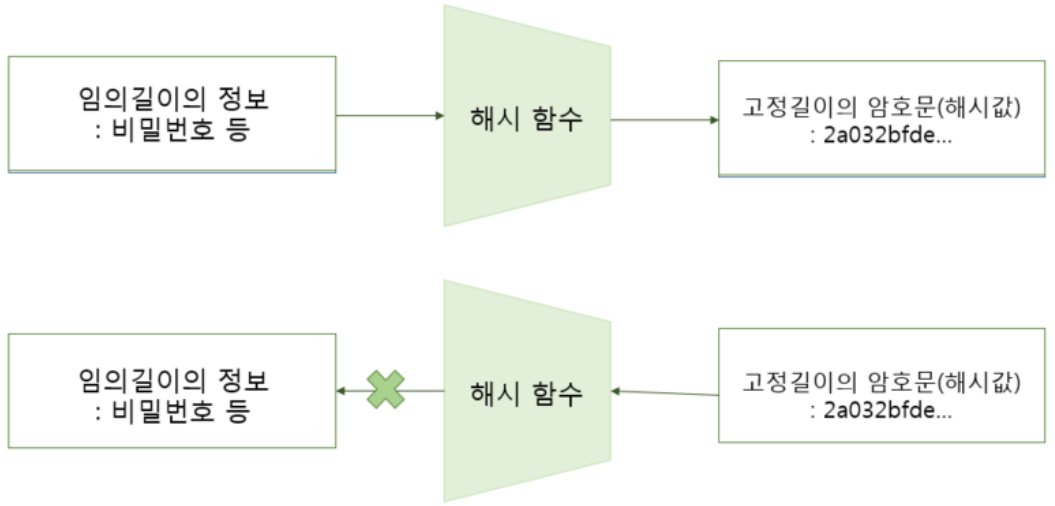
블록체인 프로토콜

- **블록체인 프로토콜(Blockchain protocol)**은 **합의 방법 (Consensus methods)**의 일반적인 용어이다.
- 이러한 방법은 블록체인 네트워크 내에서 **합의에 도달**하고 거래를 **검증**하기 위해 구현되는 **서로 다른 시스템**이라고 볼 수 있으며, 이러한 합의 알고리즘에는 PoW, PoS, DPoS, PAXOS, PBFT, Raft 등이 있다.
- 대부분의 글로벌 기업들은 이러한 블록체인 프로토콜 중 하나 또는 조합을 사용하고 있으며, 대표적인 프로토콜은 그림과 같다. 중요한 것은 이러한 합의 알고리즘은 블록체인에서 매우 중요하며, 어떤합의 알고리즘을 사용하는지는 블록체인의 기술력과 경쟁력으로 여겨지기도 한다.
- http://wiki.hash.kr/index.php/%ED%95%A9%EC%9D%98_%EC%95%8C%EA%B3%A0%EB%A6%AC%EC%A6%98



블록체인의 기술 – SHA256

- SHA-256은 SHA(Secure Hash Algorithm) 알고리즘의 한 종류로서 **256비트로 구성**되며 **64자리** 문자열을 반환한다. SHA-256은 미국의 국립표준기술연구소(NIST; National Institute of Standards and Technology)에 의해 공표된 표준 해시 알고리즘인 SHA-2 계열 중 하나이며 **블록체인**에서 가장 많이 채택하여 사용하고 있다.
- **단방향** : 단방향(One-Way) 암호화는 평문을 암호화했을 때 다시 평문으로 복호화할 수 없는 암호화이다. 대표적으로 많이 사용되는 알고리즘이 SHA-256 암호화 알고리즘이다.
- **안정성** : SHA-256의해 제공되는 **해시 알고리즘**은 일정한 컴퓨터 연산 속도의 향상을 염두에 둔 가정에도 산술적으로 매우 강력하다는 결론에 도달하게 된다. 혹여 미래에 SHA-256의 **취약점**이 발견되더라도 블록체인에는 **하드포크(Hard Fork)**와 같은 알고리즘 개선 기법들이 존재하기 때문에 취약점을 제거할 수 있다.



블록체인(비트코인) 동작원리