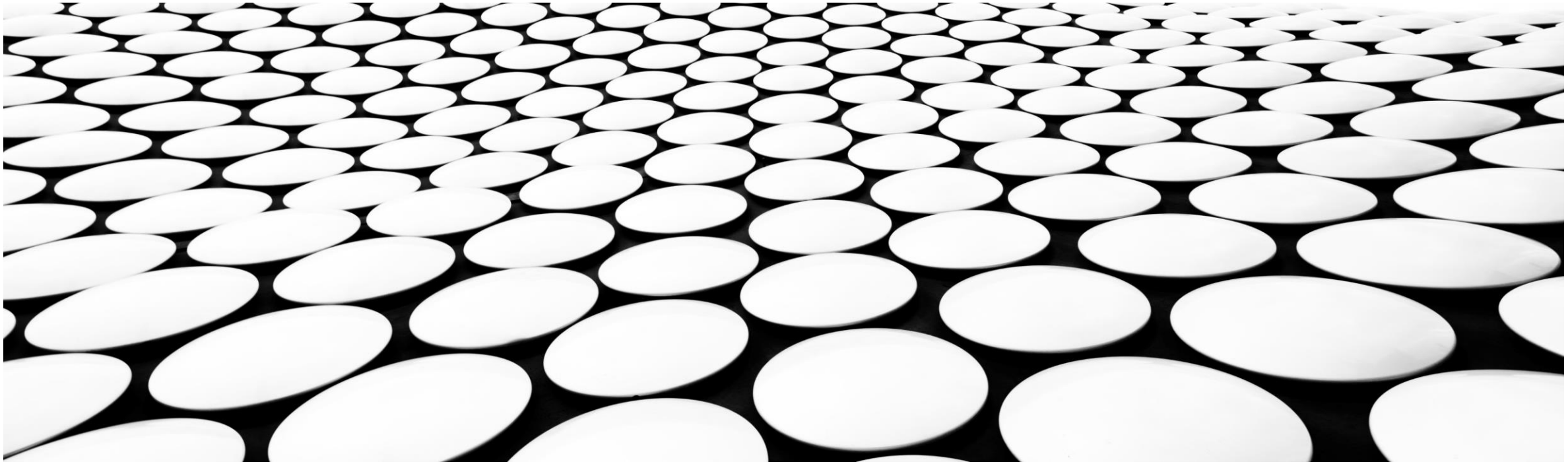
블록체인(BLOCK CHAIN)



목차

1. 블록체인의 미래와 전망

- 시장조사기관 가트너에 따르면 2020년에는 사업적 부가가치의 연간성장률이 120%에이르고, 2030년에는 사업적 부가가치가 약 3조 달러를 초과할 것으로 예측되고 있다.
- 블록체인 기술은 신뢰성 및 안정성을 바탕으로 현재 금융, 유통, 물류, 제조, 공공 서비스등 다양한 분야에 적용되고 있으며, 데이터의 보안성 및 신뢰성이 보증되어야 하는 보험, 가상화폐, 개인인증, 유통 등의 분야를 중심으로 블록체인 활용이 확대되고 있는 상황이다.
- 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 해석되어 지고 있다.

주요 국가별 현황

- 미국

정부서비스에 블록체인을 활용하기 위해 연방정부 및 주정부가 법률제정 등을 추진 하는등 블록체인에 대한 관심이 증가되고 있다.

버몬트주(2016. 6.), 애리조나주(2017. 3.), 네바다주(2017. 6.)는 블록체인 상 기록 및 서명의 법적 효력을 인정하거나 블록체인 거래에 대해 면세하는 법안을 통과시켰으며,

델라웨어주(2017. 7.)는 주식 거래 명부에 블록체인의 사용을 허용하고 있다. 또한, 나스닥 주식거래 시스템에 블록체인 기술 도입을 추진하고 있으며 연방준비은행(FRB) 주도의 블록체인 기반 지급결제 시스템 개발과 금융거래에 적용할 수 있는 플랫폼을 개발 중이다.

주요 국가별 현황

- 중국

중국은 4차 산업혁명시대의 핵심기술로 블록체인을 선정(2016. 12.)하여 기술개발 및 시범사업을 추진하고, 항저우에 블록체인 산업 파크를 조성하고 있다.

또한, 제13차 5개년 국가 정보화 계획에 블록체인을 포함시키는 등 블록체인 활성화 정책을 추진 중이며 정부-민간 형태의 블록체인 단지 건설(33조 원 투입 예정) 및 블록체인 기반의 중국 전자화폐 개발을 추진 중이며, 블록체인 특허출원(2018. 1., 특허청)도 472건에 달한다.

주요 국가별 현황

- 한국

국내에서는 중소 전문기업과 SW 및 정보통신 기업이 블록체인 플랫폼 기술력을 보유하 고 있으며, 다양한 시범사업을 통해 실증 사례를 확보하기 위한 노력을 경주하고 있다.

특히, 블록체인과 관련해서 실제 비즈니스에 적용하여 상용화하기 위해 정부 및 기업들이 적극적으로 발 벗고 나서고 있다.

먼저, 과학기술정보통신부와 한국인터넷진흥원은 국내 블록체인 산업 진흥을 위해 블록체인 시범사업을 추진하고 있다.

2019년의 경우에는 사업 대상을 민간 부문까지 확대하여 211억 원을 들여 공공 부문 12개, 민간 부문 3개 과제로 크게 확대하여 추진할 계획이다.

삼성SDS, LG CNS는 금융, 제조, 공공, 물류 등 다양한 분야에 블록체인 사업 기회를 발굴하고 블록체인 고도화를 위한 기술 개발에 나설 계획으로 있으며, SKT/KT는 블록체인 관련 전담조직을 구성하여 전자문서 관리, 모바일ID 인증 등에 블록체인 기술을 적용 중이다.

또한, 네이버 및 카카오도 블록체인 기술 자회사를 설립하여 블록체인 기술을 개발하고 있다.

최근에는 금융위원회 주도의 공동 블록체인 컨소시엄을 출범하여 국내 16개 주요 은행과 블록체인 제도화 연구를 진행하고 있다.

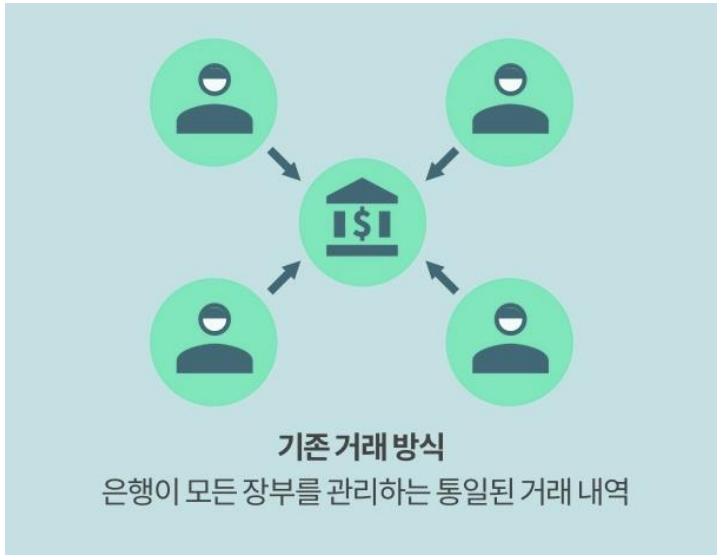
블록체인 기술 적용 사례

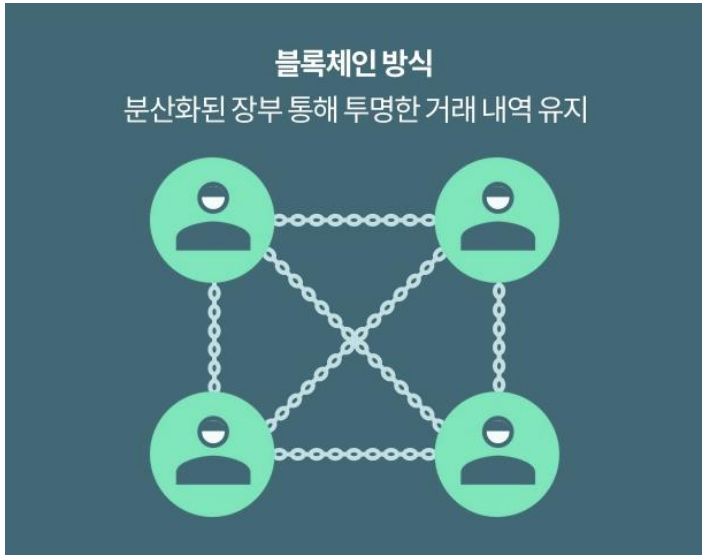
분야	대표기업	주요 내용
보안/인증	SK텔레콤	LG유플러스, 코인플러그, 해치랩스 등과 협력해 전화번호를 바탕으로 신원을 간편히 증명할 수 있는 모바일 신분증 기술 개발
	파수닷컴	블록체인 기반의 증명서 확인검증 플랫폼인 파스블록 개발
물류/유통	삼성 SDS	'넥스레저(Nexledger)' 블록체인 플랫폼을 활용하여 관세청 "블록체인 기반 수출통관 물류서비스" 시범운용
	현대글로비스	정보기술(IT) 전문기업 현대오토에버는 블로코와 손잡고 중고차 이력관리 서비스 개발
의료	매디블록	블록체인 기반으로 의료, 관광, 금융을 통합해 체계적인 의료 환경과 양질의 의료 서비스를 제공해 주는 의료관광 모바일 결제 플랫폼 '메디토' 개발
	KBIDC	블록체인을 활용하여 DNA와 RNA에 있는 핵염기 순서를 규명하고 저장하는 플랫폼인 시퀀스 마이닝플래폼(SMP) 기술 특허를 등록
금유/보험	삼성	갤럭시 S10에 전자지갑(월렛)을 탑재하여 암호화폐를 저장 및 송금할 수 있도록 하였으며, 디앱(DApp) 등 블록체인 서비스를 출시하고, 현재 블록체인 기반 신원확인 플랫폼을 개발 중에 있음
	SK C&C	하이퍼레저 패브릭 기반 프라이빗 블록체인에 리플 기반 가상화폐(암호화폐) 지급결제 시스템을갖춘 블록체인 플랫폼 '체인Z' 출시
게임	위메이드	블록체인의 데이터 분산·저장 기술이 아이템 거래 내역, 랭킹과 같은 게임 데이터를 투명하고 안전하게 관리 할 수 있는 `버드토네이도' 출시
	코드박스	고크립토봇은 캐릭터 수집, 업그레이드, 판매, 이용자간 대결(PvP) 등 게임의 다양한 요소를 이더리움 스마트 컨트랙트 기반으로 제공한다.

2. 블록체인(BLOCK CHAIN) 이란 ?

- **블록체인** 은 관리 대상 데이터를 **블록** 이라고 하는 소규모 데이터들이 P2P 방식을 기반으로 생성된 체인 형태의 연결고리 기반 분산 데이터 저장환경에 저장되어 누구도 임의로 수정될 수 없고 누구나 변경의 결과를 열람할 수 있는 분산 컴퓨팅 기술 기반의 데이터 위,변조 방지 기술입니다. 이는 근본적으로 분산 데이터 저장기술의 한 형태로, 지속적으로 변경되는 데이터를 모든 참여 노드에 기록한 변경 리스트로서 분산 노드의 운영자에 의한 임의 조작이 불가능하도록 고안되었습니다. 잘 알려진 블록체인의 응용 사례는 암호화폐의 거래과정을 기록하는 탈중앙화된 전자장부로서 비트코인이 있습니다. 이 거래 기록은 의무적으로 암호화되고 블록체인 소프트웨어를 실행하는 컴퓨터상에서 운영되고 비트코인을 비롯한 대부분의 암호화폐들이 블록체인 기술 형태에 기반하고 있습니다.
- 다시말해 블록체인은 **데이터 분산 처리 기술** 입니다. 네트워크에 참여하는 모든 사용자가 모든 거래내역 등의 데이터를 분산하여 저장하는 기술을 뜻합니다. 이렇게 저장된 데이터를 블록이라 칭하며 여러 블록들을 시간의 순서대로 묶는 형태를 가져 블록체인이라 불리게 됩니다. 이 모든 사용자가 거래내역을 보유하고 있어 거래 내역을 확인할 때는 모든 사용자가 보유한 장부를 대조하고 확인해야 합니다. 이러한 이유로 블록체인은 **공공거래장부**, **분산거래장부** 로 불리기도 합니다.

블록체인의 거래방식





기존의 거래방식은 중앙기관 즉, 은행에서 모든 거래 내역을 저장하고 있습니다.
개인 간 거래사실을 **저장** 하여 **증명** 해야 하기 때문입니다.
블록체인은 은행과 다르게 해당 네트워크에 참여한 인원이 거래내역을 나눠서 저장하게 됩니다.
만약 한 네트워크에 100명이 참여하고 있다면 개인간 거래 내역을 100개의 블록을 생성해
100명 모두에게 전송한 뒤 저장을 합니다.
후에 거래내역을 확인할 때는 블록으로 나눠 저장한 데이터들을 연결해 확인합니다.

블록체인의 특장점

- 위에서 말한 것처럼 블록체인은 **분산저장** 을 한다는 점이 특징입니다. 기존 거래방식에서는 데이터를 위,변조하기 위해선 중앙서버를 공격하면 됐습니다. 그러나 블록체인의 경우 여러 명이 동일한 데이터를 저장하기 때문에 위, 변조가 어렵습니다. 블록체인 네트워크를 위, 변조하기 위해서는 참여자의 거래 데이터를 모두 공격해야 하기 때문에 사실상 해킹이 불가능하다고 여겨집니다.
- 블록체인은 중앙 관리자가 필요 없습니다. 중앙기관이나 관리자 없어도 다수가 데이터를 저장, 증명할 수 있기 때문에 **탈중앙** 이 가능합니다.

블록체인과 비트코인

- 비트코인과 같은 암호화폐가 등장한 것도 앞에서 설명한 블록체인의 특장점 덕분입니다. 비트코인을 원하는 사람들이 직접 채굴을 통해 발행할 수 있습니다. 일각에서는 블록체인이 중앙기관과 은행을 대체할 것이라는 전망을 보여주기도 합니다.
- 암호화폐에서는 **이중지불방지**를 위해 아래와 같은 다양한 시간표시 방법들을 사용합니다. 이중지불이란 100만원의 잔고에서 돈을 100만원 출금을 한 뒤, 잔고가 0원으로 갱신되기 전 재빨리 100만원을 또 출금하는 시간차 공격을 말합니다.
- **채굴방식 (이중지불방지 방식)**
  1. 작업증명 (POW : proof-of-work)
  2. 지분증명 (POS : proof-of-stake)
  3. 위임지분증명 (DPOS: delegated proof-of-stake)
  - 대표적으로 위와 같은 방법으로 이중지불 문제를 해결하고 있습니다.

3. 블록체인의 기술 정의

- **블록체인(Blockchain)**

블록체인은 **최초의 블록**(Genesis Block) 부터 시작해서 바로 앞의 블록에 대한 링크를 가지고 있는 링크드 리스트인 자료구조 입니다. 다시 말해 블록과 블록을 체인으로 이어준 형태입니다. 블록체인에서 사용되는 블록은 일정 시간마다 생성이 됩니다. *(비트코인의 경우 10분에 한 번씩 생성)*

즉 여러 건의 거래내역을 하나의 블록으로 묶어 기존에 생성된 블록에 체인처럼 계속적으로 연결한 구조를 의미합니다. 블록의 집합체인 블록체인은 여러 노드에 걸쳐 분산되어 저장 및 관리되며 모든 거래 정보를 포함하는 거대한 분산 장부 또는 공통장부(원장: Ledger)관리 기술이라 할 수 있습니다.

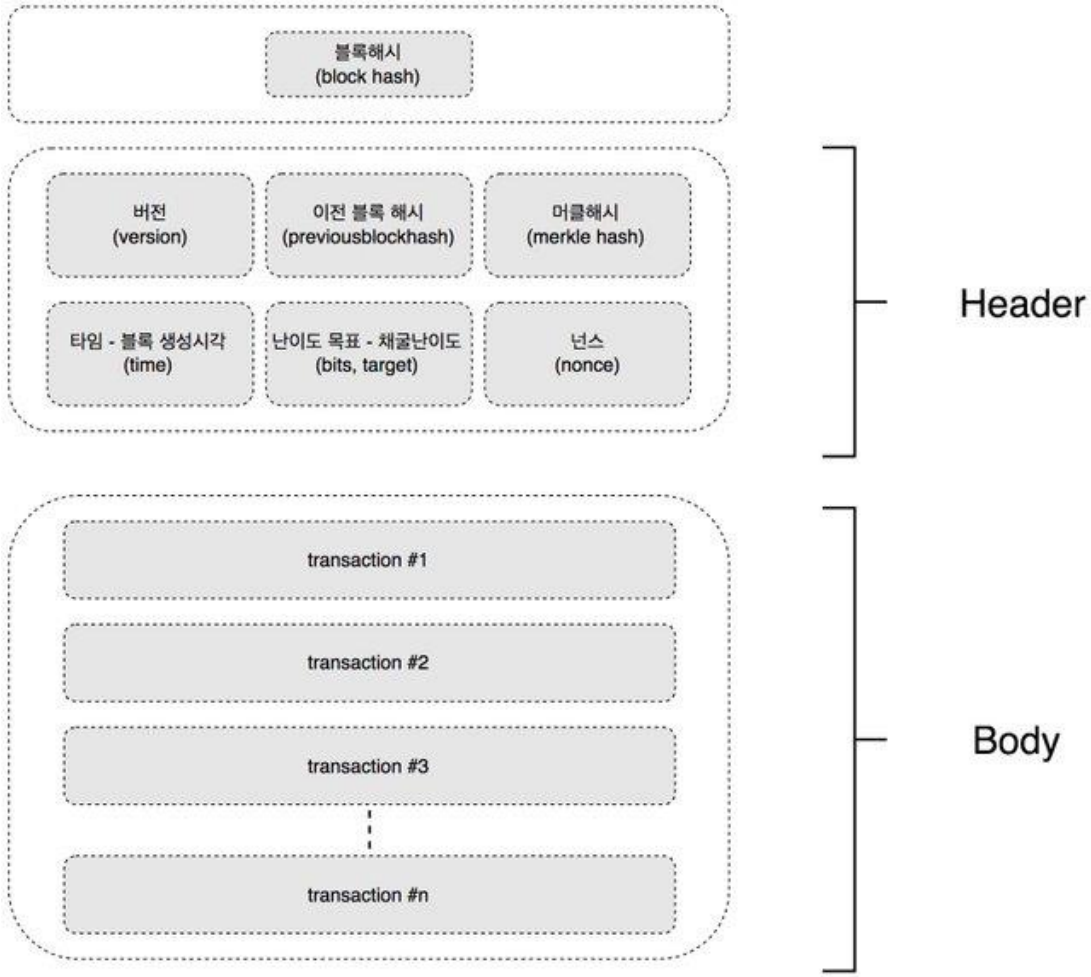
- **블록(Block)**

블록이란 **블록체인의 원소 개념으로 다수의 거래정보의 묶음** 을 의미합니다. 블록은 Height라고 불리고 있습니다. 블록체인을 길게 이어진 수평선으로 보는 것이 아니라 탑의 형태로 구성된다고 생각하여 Height라는 말을 쓴다고 합니다. 하지만 이 Height는 정확한 블록의 이름이 아닙니다. 블록의 정확한 이름은 TXID 라 불리는 블록의 해시 값입니다.
이 **블록의 해시 값은 블록의 헤더 정보를 모두 합산한 후** SHA256**으로 변환된 값** 입니다.

3. 블록체인의 기술 정의

- **블록 구성 요소**

블록은 블록 헤더와 거래 정보, 기타 정보로 구성됩니다. 여기서 거래 정보와 기타 정보는 블록 바디라 볼 수 있습니다. 거래 정보는 입출금과 관련한 여러 가지 정보를 가지고 있고 기타 정보는 블록 내에 있는 정보 중에서 블록 헤더와 거래 정보에 해당하지 않는 정보를 말하며, 블록 해쉬 계산에 사용되지 않습니다.



4. 채굴(MINING) 방식

- 리플과 같이 최초 발행 이후 추가발행이 불가능한 암호화폐도 있지만 대부분은 채굴방식을 통해 추가발행이 진행됩니다. 채굴방식은 대표적으로 POW, POS, DPOS가 있습니다.
- 한마디로 어떤 방식으로 채굴을 해서 보상을 받을것인지에 대한 **약속** 이라고 보면 됩니다. 명칭은 **채굴 증명 방식**, **합의 프로토콜**, **합의 메카니즘** 등 여러 용어로 부르기도 합니다.

작업증명(POW)

- POW(Proof of Work)
- **작업증명** 으로 부르기도 하며 해시연산을 처리하는 하드웨어(GPU, ASIC 채굴기) 등을 사용해서 증명하는 방식입니다. 간단하게 말해 하드웨어 장비를 사용해 코인을 채굴하는 것입니다.
- 해시함수에서 나온 출력 값을 채굴자들이 하드웨어 장비 (GPU, CPU와 같은 컴퓨팅 파워)를 통해 결과를 도출하는 것입니다. 여기서 해시는 단방향 암호화 기술이므로 결과값을 가지고 역으로 입력 값을 찾아낼 수가 없습니다 *(암호화된 결과에 대해 복호화가 불가능)*. 따라서 무차별 대입으로 출력 값과 똑같은 결과가 나올 때까지 실행하는 방법밖에 없습니다. 이렇게 초당 해시를 처리하는 것을 **해시 레이트**(h/s) 라 부르기도 합니다.
- 이러한 방식으로 문제를 해결하면 **가장 빨리 채굴된 블록만 인정을 받고 나머지는 버려지게 되기 때문에 이중 지불 문제가 해결** 되게 됩니다.
- 대표코인

비트코인, 라이트코인, 제트캐시, 모네로

지분증명(POS)

- POS(Proof of Stake)
- **지분증명** 이라 부르기도 하며 채굴기 없이 본인이 소유한 코인의 지분으로 채굴되는 방식입니다. 위 PoW의 단점을 극복하기위해 등장하였습니다.
- **해당 코인을 가지고 있는 소유자** 가 현재 보유하고 있는 자산(stake) 양에 비례하여 블록을 생성할 권한을 더 많이 부여되는 방식입니다. 참여에 대한 보상은 이자와 같은 방식으로 코인이 지급되며, 일정 수 이상의 코인을 보관하고 있는 지갑을 블록체인 네트워크에 연결시켜놓기만 하면 보상을 받을 수 있습니다.
- 이러한 설명으로는 채굴장비없이 **이자(해당코인)** 를 받게 되니 좋을 것 같지만 코인을 보유하고 있는 사람 누구나가 DB를 업데이트 할 수 있게 되는 방식은 위험하다고 볼 수 있습니다. 해당 코인 지분이 많은 사람이 악의적인 공격을 가하게 된다면 해당 블록체인은 위험할 수 밖에 없기 때문입니다.
- 그럼에도 PoS를 선호하는 이유

기존 PoW 방식은 블록체인의 정당성을 확인할 수 있지만 채굴 노드의 경우 하드웨어를 직접적으로 갖춰야 하고 에너지 소모가 굉장히 클 뿐더러 대량의 채굴기를 돌리는 경우 지리적으로도 넓은 평지를 가지고 있어야 가능한데 채굴기 자체에서 발생하는 열과 소음이 상당하기 때문입니다.

- 대표코인

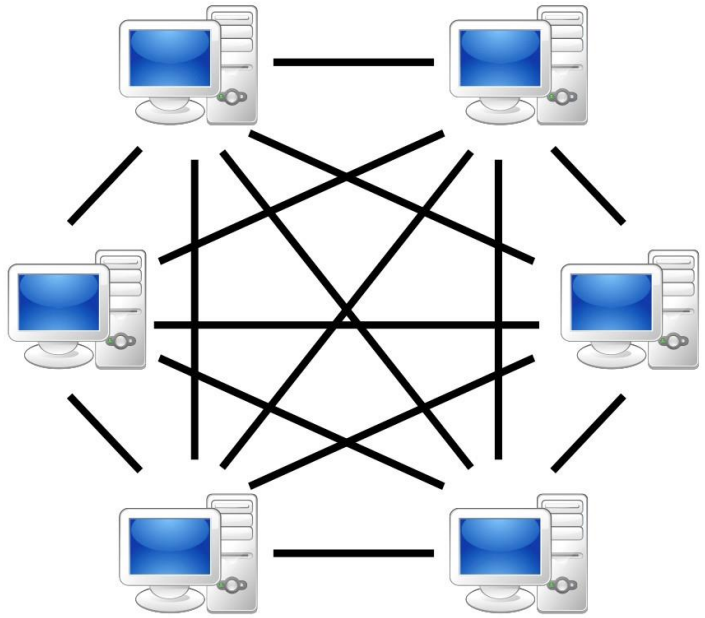
퀀텀, 네오, 스트라티스

위임지분증명(DPOS)

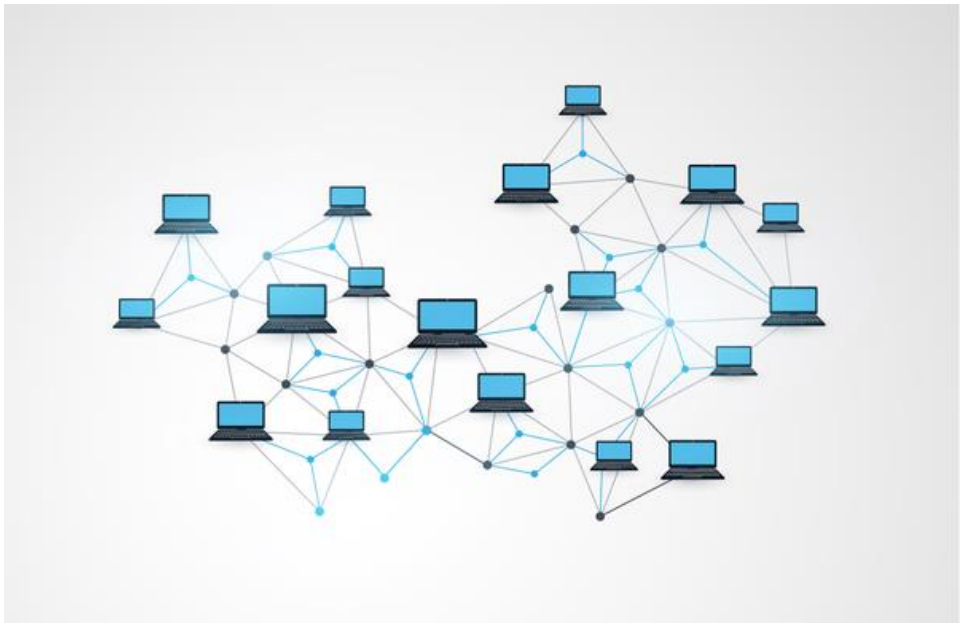
- DPOS(Delegated Proof-of-Stake)
- **위임지분증명** 이라 부르기도 하며 말그대로 위임된 POS입니다. PoS가 자산을 가진 사람들이 전부 참여할 수 있는 방식이라면 DPoS **는 특정 인원에게만 POS를 할 수 있도록 권한을 위임하는 것입니다.** 즉 특정인 몇 명만이 블록을 생성하여 증명할 수 있습니다.
- DPoS 네트워크는 구성하는 모든 노드들의 투표 결과로 정한 상위 노드에게 권한을 위임하여 일종의 대표자가 되는 것입니다. PoS의 경우, 일정 지분을 소유한 모든 노드에게 블록 생성 권한이 주어지기에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

스팀, 이오스, 아크, 라이즈

5. P2P 와 블록체인 네트워크 비교

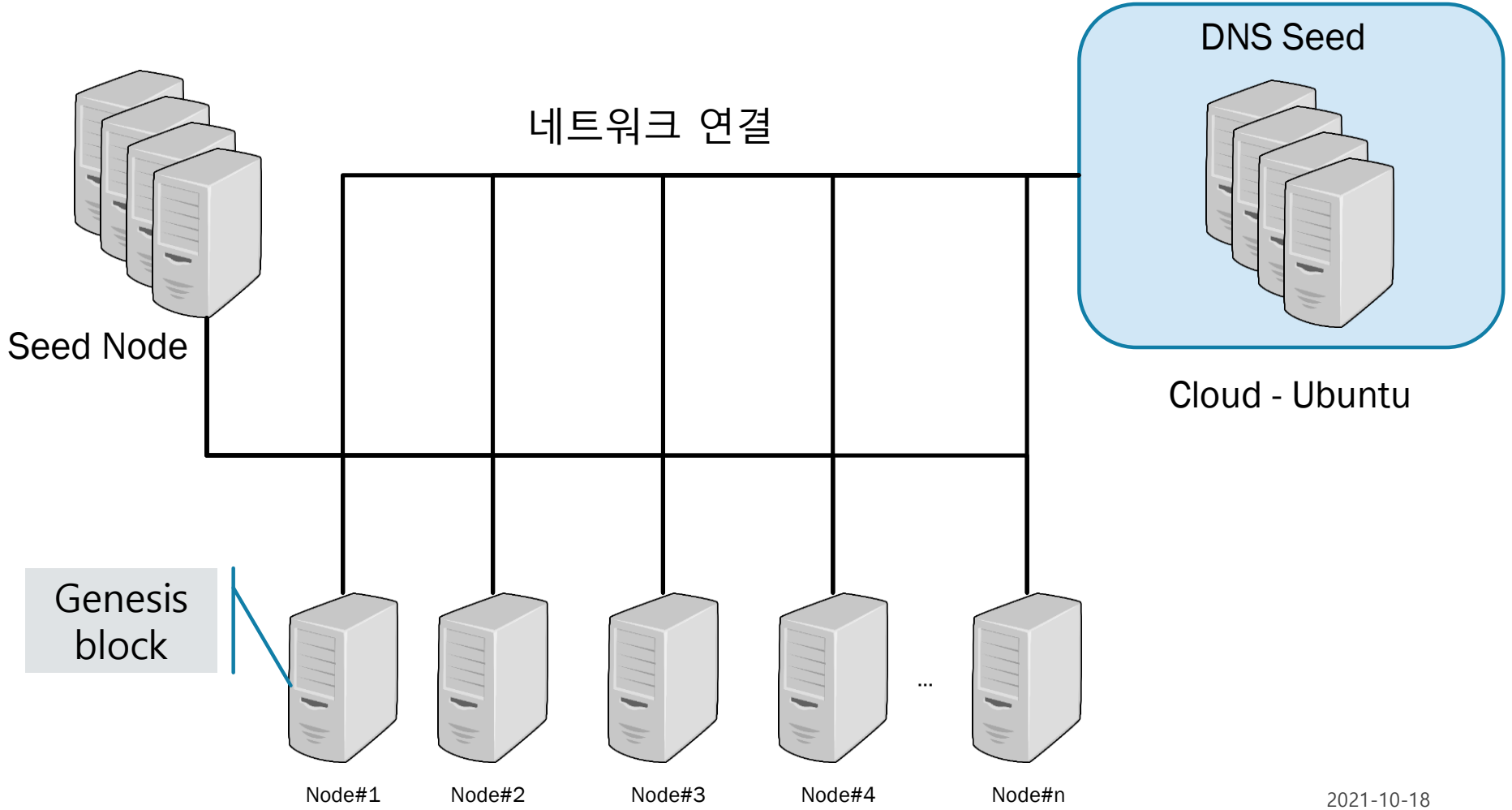


P2P-network



블록체인 network

블록체인(비트코인) 동작원리



6. 블록체인을 배워야 하는 이유

- 대부분의 사람들이 블록체인의 현재 기술수준과 향후 전망에 대해서 매우 낙관적으로 평가하고 있으며, 블록체인 분야의 전문가들도 한시라도 빨리 이 기술을 사회 전반 모든 분야에 도입해야 기술경쟁에서 뒤쳐지지 않을 것이다.
- 이에 따라 블록체인에 대해 깊게 알지 못하는 대부분의 사람들에게는 블록체인이 사회 전반의 문제를 해결 할 수 있는 만능의 기술인 것이다.
- 미래 지능정보 시스템 및 분산 사회구조 시대를 대비하여 블록체인을 금융부문은 물론 전 산업에 활용하기 위한 알고리즘, 플랫폼, 애플리케이션, 게임, IoT 적용 디바이스 및 센서 등의 기술 개발을 적극 추진하고 비즈니스 모델을 개발하여 새로운 생태계를 주도해야 한다.

7. 블록체인을 개발 하기 위해...

- 블록체인 네트워크의 운영은 꽤 많은 스킬을 요구 하고 있다.
  - 개발언어 : C/C++, HTML, Java, Java Script, Nodejs, Python, Json, XML 등
  - 개발 플랫폼 : Windows, Linux, Mac, Android, iOS 등
  - 데이터 베이스 : mysql, mssql, Oracle, redis, MongoDB 등
  - 개발 클라우드 : Amazon, Google 등