블록체인 네트워크 기반의 암호화폐 동향 분석

임세진, 김현지, 서화정
한성대학교 IT융합공학부

HSU 한성대학교 HANSUNG UNIVERSITY

CryptoCraft LAB
https://crypto.modoo.at

Contents

CryptoCraft LAB

개요

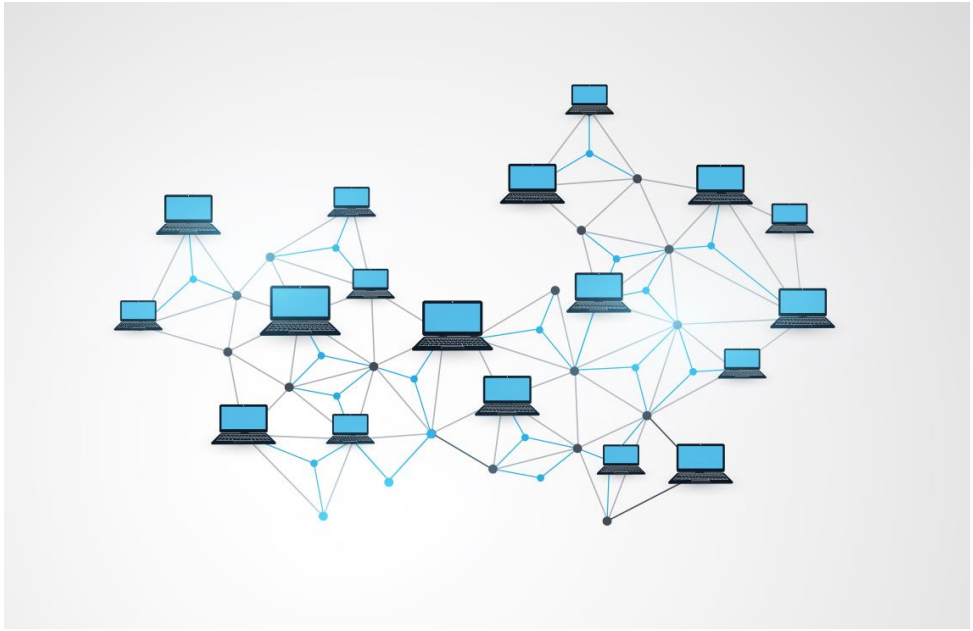
- 암호화폐(Cryptocurrency)란 ?

- 분산원장 시스템 내에서 안전하게 전송되고 해시함수를 이용해 쉽게 소유권을 증명해 낼 수 있는 디지털 자산

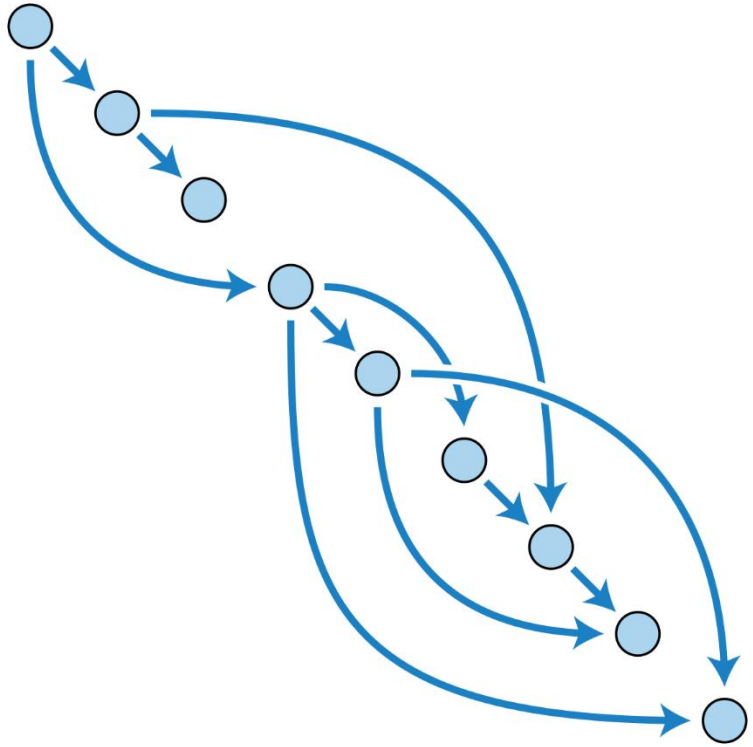
- 중앙은행 없이 전 세계의 노드에 P2P방식으로 분산 저장하여 운영

개요

- 블록체인이나 DAG를 기반으로 한 분산 원장 위에서 동작



Blockchain



Directed Acyclic Graph

비트코인 (Bitcoin) – 1세대 암호화폐

- 2009년 나카모토 사토시에 의해 개발

- 블록체인 기술로 구현한 최초의 암호화폐

- 중앙기관 없이 참여자들의 네트워크로 거래 이루어짐

- 중계기관 없는 결제 및 송금 기능 구현

  => 화폐와 은행 시스템 대체 가능

비트코인 (Bitcoin) – 1세대 암호화폐

- PoW(작업증명) 합의 알고리즘 사용

- 블록체인 네트워크 : 평균 10분마다 트랜젝션들 모아 블록 생성

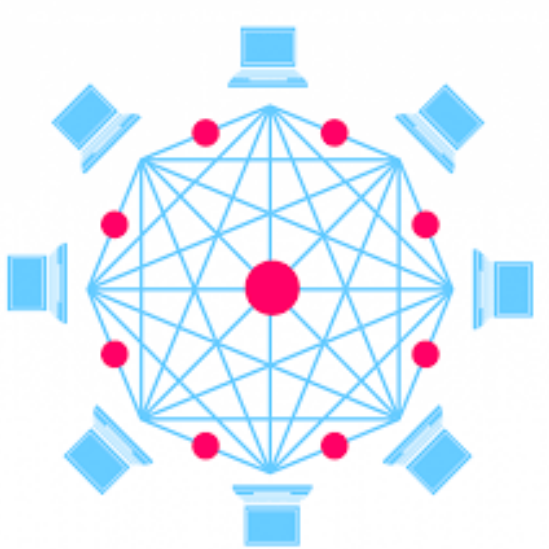
- 평균 4 – 6건의 TPS (초당 거래처리속도)

Proof of Work

비트코인의 합의 알고리즘 - PoW

비트코인 (Bitcoin) – 1세대 암호화폐

- 의의



- 분권화와 탈중앙화에 기반한 시스템 시도
- 기존 금융 시스템의 혁신

- 한계점

- 기존의 1MB의 블록사이즈 + 10분 간격의 블록 생성 시간

  => 비트코인의 거래량 증가로 인한 빠른 거래처리 불가능

- 한정된 분야, 낮은 확장성
- 모두에게 동등한 권한 부여 => 의사결정 과정에서의 합의도출의 어려움

이더리움 (Ethereum) - 2세대 암호화폐

- 2015년 비탈릭 부테린에 의해 개발

- 스마트 컨트랙트(smart contract)를 블록체인 기반으로 구현한

  최초의 암호화폐 플랫폼

- 고유의 프로그래밍 언어인 솔리디티(Solidity) 제공

  => 스마트 계약을 구현하기 위해

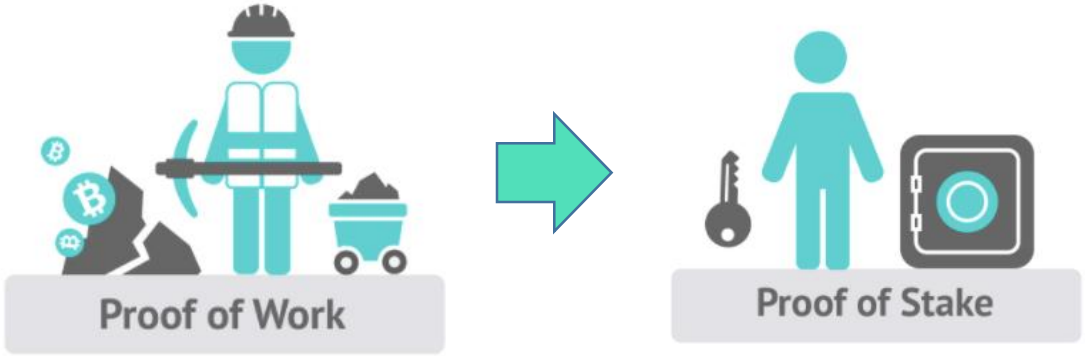
이더리움 (Ethereum) - 2세대 암호화폐

- 12초마다 하나씩 블록 생성

  가변적인 블록의 사이즈 => 비트코인보다 빠른 트랜잭션 처리

- 합의알고리즘 PoW -> PoS 전환 예정

- 평균 7 – 14건의 TPS (초당 거래처리속도)



이더리움 (Ethereum) - 2세대 암호화폐

- 의의

- 이더리움의 스마트 컨트랙트를 중심으로 계약의 자동화

- 화폐 성격이 강한 비트코인 -> 온라인 거래 플랫폼으로까지 확장된 이더리움

- 한계점

- 거래속도, 개발환경, 상호호환성, 의사결정 알고리즘

- 많은 사용자로 인한 트랜잭션 처리 상당히 느림

이오스 (EOS) 와 에이다 (ADA) – 3세대 암호화폐

- 이오스(EOS)

- 댄 라리머를 주도로하여 개발된 퍼블릭 블록체인

EOS

- 개발목적

  : 기존 블록체인 플랫폼의 비싼 수수료와 느린 트랜잭션 처리속도 개선

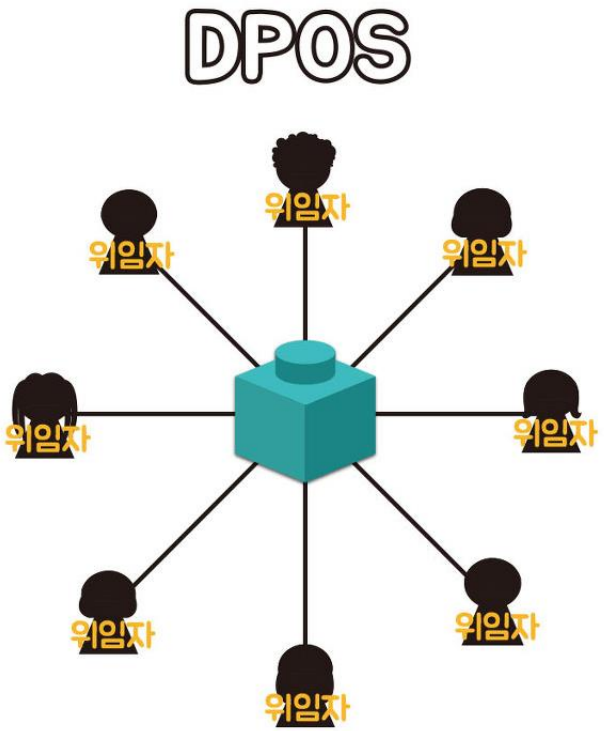
- 많은 부분을 웹 어셈블리로 개발 => 속도 개선

이오스 (EOS) 와 에이다 (ADA) – 3세대 암호화폐

- DPoS를 합의 알고리즘으로 채택

- 이오스 보유자들의 투표 -> 21명의 대표자 노드 선출 (블록 생성 권한)

- 평균 3,000건의 TPS (초당 거래처리속도)



이오스 (EOS) 와 에이다 (ADA) – 3세대 암호화폐

- 에이다(ADA)

- 기존 암호화폐들의 설계, 개발 방식 전환을 위해 등장

- 분산형 퍼블릭 블록체인 플랫폼 ‘카르다노’ 위에서 동작하는 암호화폐

이오스 (EOS) 와 에이다 (ADA) – 3세대 암호화폐

- 하스켈 언어로 구현 => 성능 및 안정성이 뛰어남

- 스마트 계약 기반의 블록체인 플랫폼

- 가장 큰 특징 : OPoS을 합의 알고리즘으로 사용

암호화폐 동향

	비트코인	이더리움	이오스와 에이다
초당 거래처리속도	4 – 6건의 TPS	7 – 14건의 TPS	3,000건의 TPS
합의 알고리즘	PoW	PoW -> PoS	DPoS, OPoS
특징	블록체인 기술로 구현한 최초의 암호화폐	스마트 컨트랙트를 블록체인 기반으로 구현한 최초의 암호화폐 플랫폼	대표 노드 선출, OPoS 알고리즘
한계점	블록 사이즈 + 블록생성시간	거래속도 + 의사결정 알고리즘	플랫폼의 한계성

이전 블록체인 기술이 가지고 있던 한계점을 보완 및 확장하는 방향으로 등장

감사합니다.