8. 블록체인

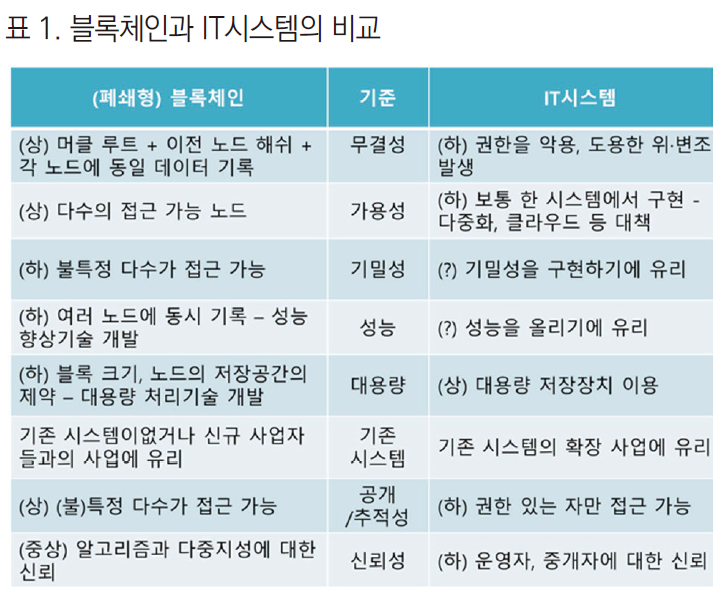
1) 필요한 이론

오늘도 당당하게 실어보는 링크  
<https://www.youtube.com/watch?v=BKLfMx5hscI>  
블록체인의 아주아주 기초적인 개념이 이해하기 쉽게 설명되어 있습니다.

블록체인의 역사

1. 2009년 익명의 개발자 나카모토 사토시가 공개한 비트코인 암호화폐의 기술  
   Bitcoin: A Peer-to-Peer Electronic Cash System
2. 실크로드: 무기나 마약 등 불법적 품목들을 취급하는 온라인 쇼핑몰  
   거래 당사자의 익명성 보장과 당사자들 간 직접적 거래를 지원하는 탈 중앙화
3. 거래소 서비스  
   암호화폐를 법정화폐로 교환하고 서로 다른 암호화폐 간의 거래를 지원  
   최초의 거래소: 마운트곡스(Mt. Gox) 원래는 게임 아이템 거래를 목적으로 설립 전세계 비트코인 거래량의 대부분을 차지하여 다양한 해킹 공격의 대상이 되어 현재는 파산
4. 비트코인의 시장 가격은 2013년 11월 경 100만 원대에서 2017년 10월 500만 원대로 증가하였고, 불과 한 달만인 2017년 11월에는 2000만 원대로 폭등하였다
5. 과열한 암호화폐 시장에 각국 정보가 규제를 걸기 시작함
6. 규제와 문제로 네임코인, 라이트코인, 모네로 등 수많은 암호화폐가 개발됨
7. 이더리움 블록체인 플랫폼 (이더 Ether 사용) 개발함으로써 단순 암호화폐 거래를 넘어 비즈니스 계약에 기반을 두었음
8. ICO(Initial Coin Offerings) 암호화폐에 기반을 둔 자금 모금 방안. 서비스 개발 계획에 대한 백서(whitepaper)-계획을 공개하고 이를 기반으로 암호 화폐를 일정 수량 투자자들에게 판매함으로써 개발 자금을 모금함 // 이더리움이 스마트 계약을 지원함
9. 2016 중반 The DAO(Decentralized Autonomous Organization) 해킹 사건  
   DAO: 모든 의사 결정이 스마트 계약(비트코인 기반 계약)에 기반을 두고 구성원들의 합의에 의해 이루어지는 조직  
   모금했으나 해킹으로 인해 10%를 잃음 -> 모든 펀드에 28일 유예 기간이 있었기 떄문에 빼내간 이더리움을 법정화폐로 인출하기 전에 하드포크를 실행하여 회복시킴  
   스마트 계약의 보안성 관심이 커졌고 DAO 특성상 해킹 발생 후 신속한 패치 대응이 어렵다는 문제가 지적됨
10. ICO가 약간의 조정을 거쳐 STO(Security Token Offerings)로 세분화되었고 법률 개정을 거쳤음

블록체인이란?

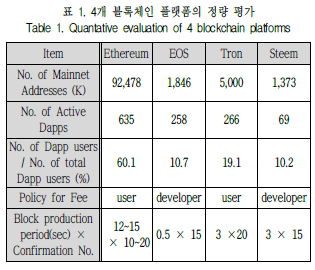
* 블록체인: PtP 네트워크로 연결되어 다수 노드에 같은 데이터를 동시에 기록하는 것  
  •투명성, 추적성 - 공개를 기반으로 한 속성  
  •공유, 협업 - 같은 데이터가 다수 노드에 동시 기록되고 공개 되기 때문에 발생되는 속성  
  •형평성, 공정성 – 공개와 추적성을 통해 공론화됨으로써 파생되는 속성  
  •무결성(위·변조 방지)에 대한 보완 - 무결성은 해쉬와 전자 서명 같은 암호 기술로 구현되지만, 노드 수가 적으면 51% 공격을 통해 위·변조될 수 있다. 다수 노드에 동시 기록되고 공개하는 블록체인의 기본 특징 역시 무결성의 기반이 된다.  
  •신뢰성 - 무결성과 공개에서 파생되는 속성  
  •기밀성(비밀성), 프라이버시: 나쁨 - 공개되기 때문에 기밀성은 나쁘다  
  •대용량 처리: 나쁨 - 같은 데이터를 다수 노드에 동시 기록하기 때문에 대용량의 저장과 처리에는 적합하지 않다. 다만 이를 개선하기 위한 다양한 기술이 개발되고 있다.  
    
  이렇기 때문에 금융업에 사용된다
* 퍼블릭 블록체인 vs 허가형 블록체인

블록 체인에 기록할 내용을 누가 읽고, 검증하며, 어떤 합의 알고리즘에 의해 블록이 선택, 기록되느냐가 블록 체인의 특성을 규정한다.

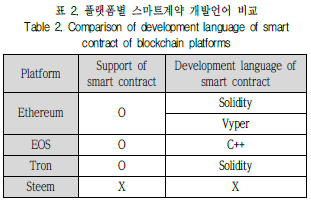
퍼블릭(비허가형)(공개형) 블록체인: 불특정 다수 누구나.

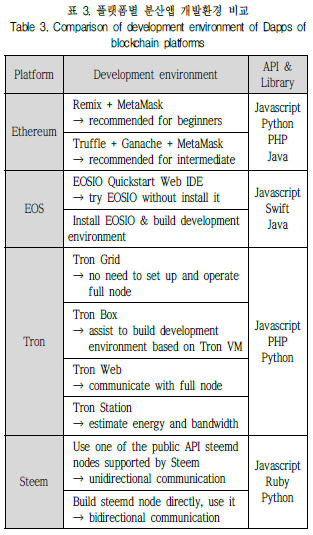
|  |  |
| --- | --- |
| 작업증명방식(PoW; Proof of Work)  누구나 합의과정에 참여하고 블록체인에 기록할 수 있음 | 비트코인, 이더리움 |
| 위임지분증명방식(DPoS; Delegated Proof of Stake)  모든 노드가 지분에 따른 권한을 소수의 노드 (이오스-블록생성자, 트론-대표자, 스팀-목격자)에 위임하고 선출된 노드들이 합의된 순서로 기록할 권한을 갖는 방식 | 이오스, 트론, 스팀, 리플 |

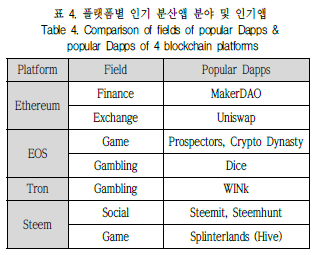
허가형 블록체인: 모든 권한이 소수의 관리자에 의해 제어됨 블록체인의 일부 장점을 희생하고 시간적, 경제적 효율성과 정보의 비밀성을 보장할 수 있음 주로 금융, 외환, 무역, 유통 관련 기업과 정부 기관에서 사용 노드들이 이 과정을 어떻게 공유하느냐에 따라 프라이빗(private), 컨소시엄(consortium) 등으로 나눈다. Ex. Hyperledger Fabric과 R3 Corda 등

2) 실생활 적용  
\*구체적인 사항은 블록체인 플랫폼 비교 논문 참고  


* 이더리움  
  언어: Solidity, Bamboo, Vyper, Flint가 있으나, Solidity, vyper가 가장 대중적이고, 예제와 매뉴얼을 이더리움 개발자 페이지에서 제공하고 있다.  
  스마트계약의 작성, 컴파일, ABI 생성 블록체인에 올리는 과정 전반을 테스트 할 수 있는 개발 툴이 있음 (여러 개 있음)  
  이더리움의 암호 화폐 Ether는 비트코인 다음으로 소장가치를 가진 금용 자산으로 인정받고 있으므로, 금용과 재정 분야의 서비스에서 가장 인기가 높다. 금융(MakerDAO)과 환전(Uniswap)에 다수의 유저 보유 중
* 이오스(EOS)  
  비트코인과 이더리움의 낮은 처리 속도와 높은 수수료를 극복함  
  스마트계약 개발 언어는 C++  
  이오스 개발자 포털에 소개되어있음 // 오픈소스 아키텍쳐 EOSIO는 CLI 기반
* 트론  
  트론의 암호 화폐 TRX  
  콘텐츠 응용서비스에 초점을 맞춘 블록체인 플랫폼 // 비트토렌트 인수  
  90% 이상의 거래량이 하이리스크 또는 도박에 치중되어있음  
  가장 인기있는 분산앱은 WINK(도박)  
  언어: Solidity. 이더리움과 호환 가능 // 트론 페이지에 상세하게 설명되어있음
* 스팀(Steem)  
  소셜 미디어 중심 플랫폼  
  스마트계약을 지원하지 않고 플랫폼 개발자들이 플랫폼 확장과 분산앱 개발툴 지원에 소극적이라는 단점  
  Steemit이라는 소셜 미디어 서비스를 블록 체인에 최초로 도입  
  콘텐츠 기반 보상 시스템; 콘텐츠를 게시하는 플랫폼 사업자 대신에, 콘텐츠 제작자와 추천자가 보상(암호화폐)를 받는 비즈니스 모델 // 이더리움과 거래 처리 속도가 빠르고 사용자 수수료가 없다.  
  스마트계약을 지원하지 않기 때문에 스팀 기반의 분산앱은 steemd 노드를 통한 RPC 호출 이용 // 개발자는 스팀이 제공하는 공용 API steemd 노드들 중 하나를 사용 – HTTPS 프로토콜을 이용한 단방향 통신만 - 하거나 직접 steemd 노드를 빌드하여 사용 – WebSockets 프로토콜을 이용한 양방향 통신 - 할 수 있다.  
  언어: 자바, 루비, 파이썬  
  7할이 SNS 사용자, 3할이 게임 사용자







3) 최신 동향

* P2P라는게 비효율적일 수 있는 동작인데 이걸 감안하고도 블록체인 방식을 활용할 수 있는 곳은 금융이다. 비싼 동작을 사용해서 신뢰성 확보가 가능하기 때문이다.
* 블록체인 대선을 아프리카에서 실시 되었다는 오보가 나오기도 했었지만, 투표 쪽에서도 사용 가능할 지도
* IoT에서도 활용할 수도 있다. 사람들끼리도 신뢰가 필요한 데, 사물끼리의 상호 작용에서 신뢰를 얻을 수 있는 방식으로 사용 가능하지 않을까? 라는 주장이 꽤 많이 나오는 중
* 블록체인과 AI의 융합. AI의 기반 데이터의 편향성을 줄이기 위해 블록체인 기반 데이터 연동 서비스에 가능성을 실는 중

[출처]

강은성. "블록체인 금융." 한국통신학회지(정보와통신) 36.7 (2019): 3-9.

박찬익. "[블록체인] 블록체인 과거, 현재, 미래." 지식의 지평 .26 (2019): 105-113.

황지연, 전민규, 김용준 and 나현숙. (2021). 블록체인 플랫폼 비교 연구. 한국지식정보기술학회 논문지, 16(2), 241-253.