블록체인 연구 관련 기초자료

주요 블록체인 플랫폼, 합의 알고리즘, dApp 현황

- Public & Private Blockchain, Distributed Ledger, dApps -

2022. 5. 13.

임명환

※ 주의 : 이 자료는 주요 블록체인 플랫폼, 합의 알고리즘, dApp을 비교 분석하기 위해 내부용으로 작성된 것임

주요 블록체인 플랫폼 및 합의 알고리즘 현황

명칭	주관	합의 방식	언어	TPS	내용 및 특징	관련 키워드
비트코인 (Bitcoin)	BTC재단	PoW	C++	4~7	・사토시 나카모토라는 저자가 2008년 10월 "Bitcoin: A Peer-to-Peer Electronic Cash System"이라는 제목의 9쪽짜리 논문을 공개(bitcoin.org)했으며, 이후 2009년 1월 3일에 세계 최초로 블록체인 기반 상용화 암호화폐인 비트코인(BTC) 탄생 ・P2P 네트워크에서 SHA-256(해시함수)으로 암호화된 수학문제인 해시를 구하여 채굴하는 작업증명(POW) 방식 ・블록 = 헤더 + 바디(평균 블록당 2,400개), 블록헤더 = 이전 블록 헤더의 해시값 + 트랜잭션 해시값 + 타임스탬프 + 논스 + 버전 + 비츠 ・공개키(Public key)-전송받을 때, 개인키(Private key)-출금할 때 ・채굴(mining) : 비트코인 네트워크에서 암호화폐의 거래내역을 기록한 블록을 생성하고 그 대가로 암호화폐를 얻는 행위 ・비트코인은 10분에 한번 새로운 블록이 생성되는데, 이 블록의 이름을 16진수로 표시한 총 64자리의 해시(hash)를 찾아내는 사람에게 비트코인을 발행하여 지급) ・비트코인 개수는 최대 2,100만개로 고정되게 디자인했으며, 채굴을 통해 10분마다 얻을 수 있는 비트코인 수가 점점 줄어드는 방식(채굴보상이 매 4년마다 절반으로 되는 반감기(半減期, halving)로 최초 블록당 50BTC에서 2020년9월 현재 6.25BTC) ・비트코인의 소스 코드를 참고하여 이더리움, 리플, 라이트코인, 대시, 카르다노, 이오스, 네오, 큐텀 등 다양한 알트코인(altcoin)들이 생겨났고, 암호통화 측면에서 비트코인은 여러 알트코인들 사이에 일종의 기축통화 역할을 하고 있음 ・2017년 8월 1일에는 비트코인 세그윗(SegWit)을 계기로 중국의 우지한이 이끄는 비트메인 등 채굴업체들이 주도하여, 기존 비트코인을 하드포크하여 새로운 암호화폐, 비트코인캐시(BCH,	사토시 나카모토, 세그윗(SegWit), SegWit2x-포기, 하드포크-비트코인캐시, 비트코인골드, 중국 규제, 반감기(매 4년)

					bitcoin cash) 출시(8월1일 10시16분에 생성된 478558 블록을 기점으로 UAHF(User Activated Hard Fork) 활성화) · 2017년 10월 24일에는 채굴에 사용되는 작업증명 알고리즘을 변경하는 하드포크로 비트코인 골드(BTG, bitcoin gold) 출시	
이더리움 (Ethereum)	이더리움 재단	PoW → PoS(예정)	C++/Go, JavaScript, Solidity	15~25	· 2015년 7월, 블록체인 기반으로 스마트 계약을 구현하기 위해 비탈릭 부테린(Vitalik Buterin)이 C++과 고(Go) 언어로 개발 · 디앱(DApp)을 배포할 수 있는 분산 응용 애플리케이션 플랫폼 · 전자화폐의 기능과 더불어 솔리디티(Solidity) 등의 튜링완전성(Turing-Completeness)을 갖춘 확장용 언어를 이용해 스마트 계약을 작성함으로 여러 분야에 접목 가능 · 20만번째 블록에서 하드포크 수행, 192만번째 블록에서 하드포크 - 이더리움 클래식(구버전) & 이더리움(신버전) 이후 3번의 하드포크 수행, 콘스탄티노플 하드포크는 실패(2018.10) · ERC-20 : 이더리움 내에서 만들어지는 토큰의 표준, 스마트 계약에 기반한 디앱은 모두 이더리움 가상머신(EVM) 환경에서 동작 · 솔리디티라는 이더리움 고유의 프로그래밍 언어로 작성된 1,000개 이상의 DApp - 트랜잭션 증가 - 속도 느려짐 · 이더해시(Ethash) 알고리즘 기반 작업증명(PoW) 방식으로 채굴 중이지만, 앞으로 작업증명 방식을 벗어나 지분증명(PoS) 방식으로 변경한 이더리움 2.0으로 전환될 예정	Dapp, ICO, 스마트컨트랙트, 솔리디티, 가상머신→웹어셈블리, GAS, 이더리움2.0(세레니티), 확장성 솔루션(샤딩, 캐스터, 레이든, 플라즈마, 플라즈마캐시), 세레니티 조합(PoS, 샤딩, 웹어셈블리)
이오스 (EOS)	block.one	DPoS	WebAssembly, Rust, C, C++ 등	3,000 ~ 5,000	· 이더리움에 비해 훨씬 더 빠른 속도와 안정성 보장, 전체 토큰 보유자들이 21명의 블록 생성자(BP)를 선출한 후 그들에게 블록체인의 운영을 맡기는 위임지분증명(DPoS) 합의 알고리즘을 채택(토큰 민주주의) · 이더리움이 평균 20TPS를 처리하는 반면, 이오스는 평균 3,000TPS의 빠른 트랜잭션 처리, 이오스 역사상 최초로 선정된 21팀의 슈퍼 노드들은 0.5초마다 1개의 블록을 생성, 득표를 받더라도 만일 24시간 동안 블록을 생성하지 못한 블록 생성자(BP)는 자동으로 지위 박탈	21팀의 BP

					• 기존 21팀의 블록 생성자들은 한 라운드 2분 6초마다 득표율에 따라 지위를 박탈당할 수 있고, 100팀의 대기 후보에 들어가게 될 수 있고, 새로운 후보가 블록 생성자 지위를 넘겨받을 수도 있음 • EOS 투표율은 대략 22% 선에서 횡보(EOS 코인 보유자가 투표를 하려면 자신의 EOS를 3일 동안 거래할 수 없게 묶어 두는 스테이킹 때문 → 자원거래소 REX(Resource Exchange)로 해결), 블록체인 간 통신을 용이하게 하도록 설계됨(활동존재증명(PoAE; Proof of Action Existence) 및 활동순서증명(PoAS; Proof of Action Sequence)을 쉽게 만들어 냄으로써 달성 • 가스(gas) 무료, 간편한 업그레이드 및 버그 복구 • 리카르디안 컨트랙트(Ricardian Contract)는 둘 이상의 당사자들이 서로 행동하기 위한 조건과 내용을 정의한 디지털 문서로서, 인간과 프로그램 모두가 쉽게 읽을 수 있어야 하고, 암호로 서명하고 승인한 것을 말함 • 대형 EOS 기축 거래소 : 비트파이넥스가 EOS 기반의 탈중앙화(DEX) 거래소 EOS파이넥스(EOSFinex) 론칭, 후오비 오픈	
하이퍼레저 (Hyperledger)	리눅스재단 /IBM				• 하이퍼레저는 스마트 계약을 구현할 수 있는 오픈소스 기반의 기업용 프라이빗 블록체인의 대표적인 프로젝트로 리눅스재단(Linux Foundation)이 주관하고 IBM이 주도적으로 활용 • 다양한 기업용 블록체인 플랫폼으로 정착시키기 위해 1) 분산원장 프레임워크, 2) 스마트 계약 엔진, 3) 클라이언트 라이브러리, 4) 그래픽 인터페이스, 5) 기타 유틸리티, 6) 샘플 어플리케이션 등이 포함된 기술표준을 제시 • 금융, 사물인터넷(IoT), 물류, 제조, 기술 등 여러 산업에 걸쳐 응용 가능한 블록체인 기술을 만드는 것을 목표로 하고 있음 • 하이퍼레저는 5개의 프레임워크(Framework)로 구성 - 하이퍼레저 패브릭(Hyperledger Fabric) - 하이퍼레저 이로하(Hyperledger Iroha) - 하이퍼레저 소투스(Hyperledger Sawtooth) - 하이퍼레저 인디(Hyperledger Indy) - 버로우(Hyperledger Burrow)	

					• 하이퍼레저는 5개의 도구(Tool)를 제공 - 하이퍼레저 첼로(Hyperledger Cello)는 맞춤형 서비스 배포 모델을 블록체인 생태계에 적용하여 블록체인 생성 관리 및 종료 시간을 최소화함 - 하이퍼레저 컴포저(Hyperledger Composer)는 블록체인 비즈니스 네트워크 구축 목적의 공동 작업 도구로 스마트 계약 개발 및 분산원장 내의 배포를 가속화함 - 하이퍼레저 익스플로러(Hyperledger Explorer)는 블록 거래, 관련 데이터, 네트워크 정보, 체인 코드, 거래 모음 및 원장에 저장된 기타 관련 정보를 열람, 호출, 배포 또는 쿼리함 - 하이퍼레저 퀼트(Hyperleger Quilt)는 주로 지급 프로토콜인 분산원장과 비분산 원장 사이의 가치 이전 목적으로 설계된 ILP를 구현하여 원장 시스템의 상호 운용성을 극대화함 - 하이퍼레저 캘리퍼(Hyperledger Caliper)는 블록체인 벤치마크 도구로 사용자가 미리 정의된 유스케이스 세트를 사용하여 특정 블록체인 구현의 성능을 측정할 수 있도록 함	
하이퍼레저 패브릭 (Fabric)	IBM/ 리눅스재단	카프카(Kafka), CFT(Crash Fault Tolerance)	자바(Java), 고(Go), 노드제이에스 (node.js)	3,000 ~ 10,000	• 스마트 계약을 구현할 수 있는 오픈소스 기반의 프라이빗 블록체인으로 허가받은 사용자만 참여(Permissioned Blockchain) • 모듈형 구조로 응용 프로그램 및 솔루션 개발의 중심 역할 • 분산원장(Distributed Ledger), 스마트 계약(Smart Contract), 합의(Consensus), 기밀성(Confidentiality), 탄력성(Resiliency), 확장성(Scalability)에 초점, 컨테이너 기술(가상화 공간에서 OS를 분할해 독립적으로 사용하는 기술)을 활용하여 시스템의 응용 프로그램 로직을 구성하는 체인코드(Chain Code) 사용 • 자바(Java), 고(Go), 노드제이에스(node.js)와 같은 범용 프로그래밍 언어로 작성된 스마트 계약을 지원하는 최초의 분산원장 플랫폼, 암호화폐 없이 합의 프로토콜을 활용 가능 • 1.4버전에서 코인 발행 가능, 노드 유형별로 네트워크 역할 할당, 병렬처리 가능	모듈형 아키텍처, plug & play, 체인코드

					• BFT적 검증은 할 수 없지만 허락된 블록체인의 성격을 적극 활용해 CA단에 위험을 1차 차단하고, 추가로 배서(endorsement) 정책을 통해 구멍 없이 보완하는 방식 • 체인코드를 통한 스마트 컨트랙트, 제어 및 감사기능이 강화된 형태로 조직간 비밀정보 유지가 용이	
하이퍼레저 소투스 (Sawtooth)	리눅스재단	경과시간증명 (PoET, Proof of Elapsed Time)	JavaScript, Python, Go, C++, Java 및 Rust		• 분산원장 구축, 배포 및 실행 목적의 모듈식 플랫폼, 블록 생성 및 검증을 가속하기 위해 트랜잭션을 병렬로 처리할 수 있는 고도의 트랜잭션 실행 엔진을 제공 • 이더리움도 지원 - 이더리움 솔리디티 자바스크립트 기반 프로그래밍 언어를 기반으로 하는 스마트 계약을 실행할 수 있는데, 이를 통해 소투스는 IDE 및 Web3와 같은 이더리움 도구를 구동할 수 있음 • 소투스-이더리움 통합 프로젝트인 세트(Seth)는 소투스 플랫폼의 상호 운용성을 이더리움으로 확장 • EVM(Ethereum Virtual Machine) 스마트 계약은 소투스 트랜잭션 패밀리를 사용하여 배포할 수 있음 • PoET - 오라클 문제를 선택적으로 해결 → 대규모 네트워크 집단 지원(IoT에 유리) • 애플리케이션 레벨과 코어 시스템 레벨 간의 명확한 분리 → 애플리케이 개발과 구축이 용이 • 전용 P2P 네트워크, 병렬 트랜잭션, 이벤트 생성 및 광고 지원, 다양한 언어를 통한 스마트 컨트랙트, 이더리움과 연동되며 퍼블릭적 요소가 가미된 하이브리드적 플랫폼	병렬 트랜잭션, seth, EVM(Ethereum Virtual Machine), 다이내믹 합의알고리즘(PoET)
하이퍼레저 인디 (Indy)	리눅스재단 소브린재단 (Sovrin)	영지식증명 (ZKP, Zero Knowledge Proof)			• 분산 개체를 위한 목적으로 설계된 분산 원장으로 인증에 특화된 프로젝트로 높은 프라이빗과 보안, 강한 아이덴티티를 위한 소프트웨어 생태계를 제공 • 상호 운용성을 위해 블록체인 또는 다른 분산원장 기반의 독립적인 디지털 개체를 생성하고 활용하기 위한 전용 도구, 라이브러리 및 구성 요소를 제공	DID (Decentralized Identity)

					• 하이퍼레저 인디는 탈중앙화된 아이덴티티가 하이퍼레저 컨소시움 내외에서 문제없이 통용되도록 하기 위한 스펙, 용어, 디자인, 패턴 등을 연구 • 인디는 거래에 대한 접근 가능한 프로비넌스(Provenance)를 제공하고, 식별자에 대한 검증 가능한 클레임을 지원할 뿐만 아니라 클레임이 더 이상 사실이 아닌 경우에 대한 철회할 수 있는 모델을 가지고 있으며, 인디가 식별자에 대한 보편적 플랫폼 역할 • 또한 인디는 DID(Decentralized Identity)를 중심으로 설계한 최초의 분산형 원장 기술로서, DID는 중앙집중식 레지스트리 서비스가 필요 없는 장기적인 디지털 ID를 가능하게 하는 새로운 형태의 디지털 식별자이며, 인디는 아이덴티티에 대한 불필요한 공개를 피하기 위해 영지식 증명(ZKP, Zero-Knowledge Proof)을 기반으로 하고 있음	
하이퍼레저 이로하 (Iroha)	리눅스재단	비잔틴 장애 허용(BFT)			• 분산원장 기술을 필요로 하는 인프라 프로젝트를 간단하게 통합할 수 있도록 설계된 비즈니스 블록체인 체계로 기본 암호화폐 없음 • 대신 시스템 상호작용 허용, 이로하는 모든 명령, 쿼리 및 네트워크 가입에 대한 사용 권한을 설정할 수 있는 강력한 사용 권한 시스템을 갖춘 유일한 원장 • 하이퍼레저 이로하는 대학, 학교 및 의료 기관과 같은 다중 인증 기관을 시스템에 통합하여, 유연한 권한 모델을 통해 ID를 인증하고 인증서를 부여할 수 있음 • 국제적 거래 - 다중서명계정을 사용 빠르고 명확한 무역 및 결제 • 금융 어플리케이션 - 감사 과정에서 매우 유용(Iroha-API 감사) • ID 관리 - KYC(Know Your Customer) 기능을 통해 다양한 애플리케이션과 완벽하게 상호작용 • 공급망(Supply Chain) 시스템 - 이로하에 사용되는 인증 시스템을 통해 물리적 항목을 토큰화하고 시스템에 통합할 수 있음 • WSJ(Wall Street Journal) 코인(2018.10.3.)	

하이퍼레저 버로우 (Burrow)	리눅스재단 모낙스 (Monax)/ 인텔(Intel)	BFT 텐더민트 프로토콜	GO		• 버로우는 이더리움 사양에 따라 스마트 계약 코드를 실행하는 허가된 블록체인 노드이고 어플리케이션별 최적화를 염두에 두고 다중체인을 위해 구축 • 노드로서 버로우(Burrow as a node)는 컨센서스 엔진, 허용된 이더리움 가상 머신 및 RPC 게이트웨이의 세 가지 주요 구성 요소로 이루어져 있음 • 스마트계약 어플리케이션은 ABCI(Application Blockchain Interface)에 대한 합의 엔진과 연결 • 승인 가능한 스마트 계약 장치 • 모듈식 블록체인 고객에게 이더리움 가상 기계(EVM)에 내장된 권한있는 스마트 계약을 해석	다중체인, REST, JSON-RPC
넥스레저 (Nexledger)	삼성SDS	컨소시엄 블록체인 (Consortium blockchain) 또는 프라이빗 블록체인 (Private blockchain)		10,000 ~ 100,000 (가속기)	• 기업용 범용 플랫폼, 블록체인 신분증과 Payment 서비스로 보안성 강화, 실시간 대량거래, 스마트 계약, 관리 모니터링 체계 등을 갖춘 블록체인 플랫폼으로 금융, 제조, 물류, 공공에 적용 • 허가된 참여자의 데이터만 검증하면 되기 때문에 매우 빠른 속도 • 거래처리속도 개선을 위해 가속기술 개발-하이퍼레저 패브릭에 적용 가능, 삼성SDS는 블록체인 플랫폼 업체 '미디움'의 블록체인 기술을 '넥스레저 유니버셜'에 적용할 예정으로 하이퍼레저 캘리퍼(Hyperledger Caliper) 기준 초당 10만 TPS 이상을 구현 • 분산 데이터와 애플리케이션 API를 표준 컨테이너 단위로 제공하여 제약 없는 글로벌 확장이 가능하며, 운영 및 유지보수 효율성이 매우 높음 • 지불결제, 인증보안, 진위증명 뿐만 아니라, 기관간 거래, IOT 등 다양한 서비스를 블록체인 플랫폼 상에서 신속히 구축함으로써, 지역, 채널, 업종의 제약이 없는 글로벌 플랫폼 생태계를 형성하여 높은 확장성 구현 • 삼성SDS는 실시간 처리 기술, 지문과 홍채 등을 이용한 생체인증을 통해 보다 완성도 있는 블록체인 플랫폼을 완성	분산원장(DLT , Distributed Ledger Technology), Digital Identity, Digital Payment, Digital Stamping 가속기술

클레이튼 (Klaytn)	카카오	BFT (Byzantine Fault Tolerance)		4,000	・카카오의 자회사 그라운드X가 개발한 디앱(dApp)을 위한 글로벌 퍼블릭 블록체인 플랫폼 ・그라운드X(2018.3 설립)는 IT 강국인 한국의 기술로 글로벌 자체 블록체인 플랫폼인 클레이튼(Klaytn)을 개발 ・15개 국가의 51개 서비스가 운영되고 있음 ・이더리움에 비해 탈중앙화를 약화시키는 대신 디앱에 필요한 실용성을 강화(블록 생성/확정 시간 1초, ETH대비 수수료 1/10) ・일반 사용자들에게 친숙한 UI, UX 디자인과 엔터프라이즈급 애플리케이션, 스테이블한 토큰 구조 등으로 설계된 새로운 형태의 블록체인 플랫폼 ・스마트 계약 실행과 외부 메모리 조작을 구분하는 가상머신인 "KLVM(Klaytn VM)" ・클레이튼은 DES 애플리케이션과 소프트웨어를 단계별로 배포 ・초기에 클레이튼 호환 디앱을 위한 IDE(Integrated Development Environment)와 일반 디앱과 EP 개발을 위한 SDK(Software Development Kit)를 출시-생태계 확장 ・블록생성에 대한 보상 - 클레이/TPS를 높이기 위해 '서비스 체인' 개념을 도입하였고, 클레이튼에서 연동되는 토큰은 '클레이(Klay)'로 사용자들은 카카오톡 내 다양한 활동을 통해 클레이(Klay)를 얻어 거래소에서 자유롭게 환전하며 활용 ・그라운드X는 클레이튼의 메인넷으로 퍼블릭 블록체인 사이프러스(Cypress)를 공개했으며(2019.6.27), 블록 생성과 확정 시간이 1초로 다른 블록체인에 비해 대기시간을 낮추고 확장성을 높여 대중화를 목표로 서비스 제공 ・클레이튼은 토큰 보관과 전송을 위해 다양한 S/W, H/W 월렛 지원 - S/W Wallet : Klaytn Wallet, Klip, Kaikas - H/W Wallet : KlaytnPhone, NFC Card Wallet	서비스 중심 플랫폼, 사이프러스, 뷰티 커뮤니티 앱 코스미(Cosmee)-첫번째 디앱(코스모체인), 레인저 노드(읽기) & 합의 노드(쓰기)
코다 (Corda)	R3				・R3(알쓰리)는 세계 최대의 블록체인 컨소시엄(80개 이상 금융기관)이고, 코다(Corda)는 R3가 만든 분산원장 기술	

					• 코다가 블록체인의 한 종류인지에 대한 여부는 끊이지 않고 있는데 코다는 블록체인이 아닌 분산원장 기술 • 코다는 블록체인 기술이 아닌, 분산원장 기술로서 기본적으로 금융산업에 최적화된 기술 • 거래당사자 간의 합의를 통해서 계약 상태의 변화를 동일하게 기록 및 보관하는 분산DB 기술, "공개된 공유 네트워크이지만, 여전히 승인된 사람들만 볼 수 있는 보안이 뛰어난 프라이빗 플랫폼" • 코다의 원장은 일부의 데이터를, 제한된 참여자에게 전파하기 때문에 기본적으로 각 노드의 관점에서 매우 주관적이고 자신과 관련 있는 정보에 대해서만 보관 • 코다의 원장은 크게 on-ledger와 off-ledger로 나뉘는데, 이는 데이터가 안과 밖, 양쪽에서 관리될 수 있음을 의미하며, 데이터가 원장의 안에 기록되어 있다고 해서 데이터가 누군가와 공유되고 있다는 것을 뜻하지는 않지만, 누군가와 공유되고 있는 데이터라면 반드시 on-ledger에 기록되어야 하며 마찬가지로 원장의 밖에 기록된 정보는 반드시 혼자만 관리되어야 함	
쿼럼 (Quorum)	JP모건		래프트 프로토콜 (RAFT protocol) 또는 이스탄불 BFT (Istanbul BFT)		• J.P. Morgan이 빠른 처리 속도를 구현하기 위해 이더리움을 하드포크하여 개발한 기업용 블록체인 플랫폼 • 쿼럼은 특정한 블록의 트랜잭션 해시를 선택적으로 볼 수 있게 하기 때문에 프라이빗 블록체인이라 할 수 있으며, 승인된 참가자만 노드로 참여, 채굴비용 및 인센티브 부존재, 개별적 노드가 퍼블릭 및 프라이빗 데이터에 대해 분리된 머클트리(Merkle Tree)를 유지하고 서로 진화할 수 있도록 설계 • 쿼럼은 풍부한 오픈소스 툴과 통합되고 엔터프라이즈 고객들이 요청한 일부 노드끼리만 특정 데이터를 공유할 수 있게 하는 컨피덴셜 트랜잭션 기능을 지원하는 점이 마이크로소프트가 쿼럼을 지원하게 된 가장 큰 요인이었음 • 마이크로소프트뿐만 아니라 스타벅스, 루이비통, MS 엑스박스 재무팀이 쿼럼을 사용	자바(Java) 기반의 테세라(Tessera) 정족수, geth(Go-Ethereum)

리플 (Ripple)	리플랩스	리플 프로토콜 합의 알고리즘 (RPCA)	C++	1,500	・2004년 핀테크 기반 리플페이(RipplePay)로 출발, 2013년 블록체인 기반 리플랩스(Ripple Labs)로 변경, 크리스 라슨(Chris Larsen)과 제드 맥케일럽(Jed McCaleb)이 암호화폐 XRP를 공동 개발, 타원곡선 디지털서명 알고리즘(ECDSA)을 사용하며, 채굴이 없이 합의에 의해 운영 ・리플 프로토콜 합의 알고리즘(RPCA)은 네트워크의 정확성과 합의를 유지하기 위해 알고리즘은 모든 노드에서 몇 초마다 적용 ・일단 합의에 도달하면 현재 원장이 마감되어 '최종 마감된 원장'이 되고, 합의 알고리즘이 성공적이고 네트워크에 포크가 없으면, 네트워크의 모든 노드에 의해 유지되는 '최종 마감된 원장'이 가장 최근의 원장으로 네트워크의 현재 상태를 나타냄 ・XRP 원장 프로토콜은 합의 및 유효성 확인을 위한 규약으로서 XRP 원장은 몇 초마다 새로운 원장 버전을 가지고 이력 형성 ・세계 여러 은행들이 실시간으로 자금을 송금(Bank2Bank)하기 위해 사용하는 프로토콜 겸 암호화폐 ・은행, 결제 서비스 제공업체, 디지털 자산 거래소를 리플넷(RippleNet)으로 연결하여 글로벌 송금 서비스 제공 ・리플 총발행량 1,000억개, 거래시간 4초 이내(XRP)	통화변환(FX) 및 지불 인계 서비스(deliver payments) xCurrent, xRapid, xVia
스텔라루멘 (Stellarlumen)	스텔라	스텔라 합의 프로토콜 (SCP, Stellar Consensus Protocol), 연합 비잔틴 동의(FBA; Federated Byzantine Agreement)	C, C++	1,000	・리플(Ripple) 공동 개발자이자 암호화폐 거래소 마운트곡스(Mt. Gox)의 창업자인 제드 맥케일럽(Jed McCaleb)이 2014년 암호화폐를 기반으로 하는 스텔라 네트워크(stellar.org)를 조이스 김과 함께 공동 설립 ・리플에서 하드포크, 국제송금, 은행, 결제 시스템, 사람을 연결하는 플랫폼, 수수료 최소 ・스텔라루멘 총발행량 1,000억개, 거래속도 2~5초 ・탈중앙화 된 리플 성격으로 스텔라 합의 프로토콜인 SCP(Stellar Consensus Protocol)는 FBA(Federated Byzantine Agreement)	국제송금/다중 통화거래

					라는 합의 알고리즘을 기반으로 개발 • SCP는 사용자가 누구를 신뢰할 것인지 직접 선택하고 이를 바탕으로 형성된 신뢰망을 이용하여 합의에 도달하는 방식 • 쿼럼(Quorum)과 쿼럼 슬라이스(Quorum Slice) 개념 도입, 쿼럼 슬라이스는 어떤 동의에 이르기 위한 일반 노드들의 집합이자 쿼럼의 하위 집합이며, 그리고 결정되어 결코 변할 수 없는 합의가 쿼럼으로 즉, 신뢰할 수 있다고 선택된 노드 집단을 의미 • 기존의 금융권을 상대로 협력관계를 만들고 있는 리플과 달리, 스텔라는 현재 은행 시스템이 구축되지 않은 개발도상국의 사용자들에게 저렴하고 편리한 소액결제 금융 서비스를 주고자 함 • IBM은 스텔라 기반의 스테이블 코인 '스트롱홀드 USD' 예정 • 다중 통화거래 가능(나이지리아 5개 통신사 연결하여 송금) • 수수료 최소화 및 최소 계정잔액 요구 • 매년 총액의 1% 추가 발행-인플레이션형 화폐	
아이콘 (ICON)	아이콘루프	루프장애허용 (LFT; Loop Fault Tolerance), PBFT		15	• 초연결성(Hyper connectivity), 스마트 계약를 지원하는 고성능 엔터프라이즈 블록체인을 목표로 개발되었으며, 다른 독립적인 블록체인과 연계를 통해 블록체인 네트워크를 확장할 수 있음 • 아이콘의 루프체인 기술은 루프장애허용(LFT; Loop Fault Tolerance) 합의 알고리즘을 기반으로 스마트계약 시스템을 지원하며, LFT는 기존 비잔틴 장애 허용(BFT; Byzantine Fault Tolerance) 알고리즘을 아이콘 네트워크 특성에 맞게 개선한 것임 • 스피닝(spinning) 기법을 사용하여 매 블록을 생성할 때마다 리더를 교체해서 장애 요소를 줄였으며, 하이퍼레저 패브릭 및 코다에 비해 스마트계약 버전 지원, 장애허용, 트랜잭션 커스터마이징이 가능 • 아이콘은 퍼블릭 블록체인 플랫폼을 표방하고 있으나, 실제 아이콘 기반의 디앱이 거의 없거나, 있더라도 트랜잭션이 거의 없다는 비판(썸씽, 위블락, 스테이지, 디스커버엑스, 메카코인 등 10여개 디앱 출시)	스코어(SCORE,Smart Contract on Reliable Environment) - 스마트 계약 플랫폼

					· 트랜잭션 개수가 거의 없다는 것은 아이콘 플랫폼 기반의 실사용자가 거의 없다는 뜻으로서, 아이콘 토큰을 가지고 있더라도 실제 사용할 곳이 없다는 의미 · 아이콘은 정부와 지방자치단체 및 금융기관 등의 블록체인 사업을 수주하여 아이콘 기반의 프라이빗 블록체인을 개발하여 납품하고 있으나, 정작 퍼블릭 블록체인 플랫폼 개발은 매우 느리게 진행되고 있음 · 최근 아이콘루프는 자체 분산신원증명 기술인 MyID를 개발하고 얼라이언스를 구성하였으며, 금융서비스에 특화된 블록체인 기반 신원인증 플랫폼을 구축하여 서비스 제공	
에이치닥 (Hdac)		균형작업증명 (ePoW, equilibrium Proof of Work)			· 현대BS&C가 사물인터넷(IoT) 플랫폼에서 사용하기 위해 만든 탈중앙화 자율기업용 암호화폐 · 퍼블릭 블록체인 메인넷에 다수의 프라이빗 블록체인이 사이드체인 형태로 복수로 연결되는 방식 · 프라이빗 블록체인은 사용자 인증뿐만 아니라, 다양한 사물인터넷 디바이스 간의 상호인증, 작동내역의 기록, 그리고 사물인터넷 계약이 수행되도록 구성 · 여기에 기 운영 중인 퍼블릭 블록체인과 상호작용을 해야만 실질적인 편리성이 높아진다 · 프라이빗 블록체인과 퍼블릭 블록체인을 상호 연결되도록 구성함으로써, 통상적인 사용자 측면과 특정한 용도로 구성된 프라이빗 블록체인이 효과적으로 사용할 수 있는 신뢰기반 생태계를 조성 · 퍼블릭 블록체인의 피투피 트랜잭션이 가능하며, 프라이빗 블록체인에서 작동하는 사물인터넷 디바이스 간의 상호 계약 및 트랜잭션을 위한 에이치닥 토큰(Hdac*T)을 구현한 플랫폼을 제공 · 이러한 기술로 사물인터넷 환경을 만족시키며, 사물인터넷 장치 간의 상호인증과 사물인터넷 계약 및 소액결제까지 모두 호환해 구현 가능	

					· 균형작업증명(ePoW) : 한 번 채굴에 성공한 노드는 일정 기간 강제로 휴식을 취하도록 만들어 다른 노드들에게 채굴 기회를 공평하게 나누어 주는 방식의 합의 알고리즘	
월튼체인 (Waltonchain)	WTC	월튼기여증명 (WPoC: Waltonchain Proof of Contribution = PoW+PoS+PoL) *PoL(노동증명)			· 블록체인 기술을 RFID 기반의 사물인터넷(IoT) 분야에 적용한 암호화폐 프로젝트 (RFID: Radio Frequence Identification) · 전자태그(RFID) 기술과 블록체인 기술을 융합한 가치사물인터넷(VIoT : Value Internet of things)을 구현해 IoT기술의 문제점을 해결하고자 함 · ERC-20 토큰, 스마트 계약 가능 · 모체인(Parent chain)&자체인(Child chain) - 확장성&트랜잭션의 과부화 해결 도모 · 모체인-60초에 한 번씩 발행된 월튼코인의 모든 거래 내용을 블록에 기록하고 이를 네트워크로 연결 · 다양한 자체인의 발행을 통해, 각 IoT 노드를 응용한 비지니스 생태계를 확장	
앤드어스체인 (Anduschain)		deb 합의 알고리즘			· 기존 합의 알고리즘의 문제점을 개선하여 개발한 deb 합의 알고리즘을 이더리움 플랫폼에 접목시킨 퍼블릭 블록체인 플랫폼 · 앤드어스체인은 이더리움이 가지고 있는 토큰 발행 기능, 스마트 계약 기능, 스마트 자산 및 DAO의 기능을 모두 가지고 있으며, 누구나 공정한 채굴 기회, 포크가 발생하지 않음 · 유료 채굴 리그, 최대 논스 규칙 및 다수결 원칙의 3가지 기본 원리 · 신뢰성을 높이는 여론조사, 스포츠 커뮤니티 서비스, 중고자동차 매매(이력관리) 서비스 등 활용을 추진	
심버스 (SymVerse)		거부권을 포함한 투표방식의 BFT			· 게임이론을 기반으로 설계·개발한 차세대 블록체인 플랫폼을 위한 암호화폐이며, 디앱 확산에 최적화된 다기능 멀티 블록체인 · 다기능 멀티 블록체인으로 속도와 용량의 문제들을 해결하며 범용거래처리기의 장착으로 소상공인들이 쉽고 편리하게 사용할 수 있게 설계	네트워크 증명 (PoN ; proof of network)

					· 거부권을 포함한 투표방식의 비잔틴 장애 허용(BFT) 방식을 채택한 가장 빠른 비잔틴 장애 허용 합의 알고리즘 · 악의적 노드의 조작방지 · 다중 블록체인은 심체인(SymChain)이라 부르며 여러 개의 블록체인으로 데이터 구조가 분산 · 그러므로 개별적인 데이터 블록의 생성시간 간격을 다르게 할 수 있고 빠른 검색처리 속도를 구현	
알고랜드 **(Algorand)**		무허가형 순수 지분증명 (PPoS)	GO,JAVA		· 블록체인의 트릴레마인 탈중앙화, 확장성, 보안성의 3중 딜레마를 해결하기 위한 플랫폼을 위한 암호화폐 · 1,000명의 검증위원들을 구성- 위원들은 블록체인에 참여한 노드들 중에서 무작위로 선발되고 선발 확률은 자신이 보유한 토큰 개수에 비례해 높아짐 · 검증 위원은 비밀리에 선발. 선발된 노드가 누구인지는 노드가 블록을 생성하고 네트워크에 전파한 이후 공개. 공개된 직후에는 또 다시 새로운 위원회가 무작위로 선발(무규칙) · 블록 생성이 1,000만분의 1초마다 이뤄지고 매번 1,000명이 참여하는 위원회 구성이 바뀌기 때문에 공격당할 틈이 없음 · 채굴에 따른 보상 없으며 무허가형-누구나 승인 필요 없이 참여 가능 · 비탈릭 부테린은 알고랜드에 대해 이더리움은 인센티브를 정면에 내세운 방식을 취하고 있다며 인센티브가 없다면 네트워크가 제대로 운영될 수 없다고 말했음	
아르고 **(Aergo)**	블로코	위임지분증명 (DPOS) 하이브리드			· 퍼블릭 또는 프라이빗, 퍼블릭 + 프라이빗 통합 구성의 모든 조합으로 사용할 수 있도록 설계한 하이브리드 방식 · 아르고는 1) 스마트 컨트랙트를 탑재한 개방형 프로토콜인 '아르고체인', 2) 블록체인 기반 서비스 구축 및 운영에 필요한 컴퓨팅 파워와 다양한 개발 툴을 활용할 수 있는 ' 아르고허브', 3) 소프트웨어 애플리케이션과 개발 요소를 사고팔 수 있는 '아르고 마켓플레이스'로 이루어져 있음	

					• 디앱 개발자와 클라우드 서비스를 제공하는 파트너 그리고 기업들로 구성된 생태계를 지원하는 기술 및 운영 프레임워크 구축 • 아르고는 빠른 성능과 안전성, 쉬운 사용성을 두루 갖춘 퍼블릭 블록체인을 중심으로 구축된 분산형 생태계를 지향 • 아르고 주요 기능은 데이터 저장을 위한 SQL, 사이드체인 기술 그리고 DPOS 합의 알고리즘 등	
체인링크 **(Chainlink)**	스마트 컨트랙트 닷컴	PoW			• 블록체인의 스마트 계약을 블록체인 외부의 데이터, 결제, API 등에 연결하기 위해 사용하는 블록체인 미들웨어 플랫폼이자 암호화폐(화폐 단위는 LINK) • 체인링크는 이더리움 기반으로 작동하는 각종 스마트 계약이 현실 세계의 데이터와 쉽게 연결되도록 돕는 역할을 하는 오라클 문제(oracle problem)를 해결하기 위한 중간자(middleware) • 체인링크는 외부 데이터를 내부로 가져올 때 발생할 수 있는 다양한 문제들을 보완하기 위해 스마트 계약을 통한 탈중앙화 방식을 채택하였으며, 스마트 계약은 3가지 기능을 수행 1) 첫째, 평판시스템(Reputation Assessment)이다. 평판 시스템은 체인링크 네트워크의 오라클 서비스 사용자들은 스마트 계약을 통해 오라클 서비스를 통해 전달받고자 하는 매개 변수의 범위를 제출한다. 해당 스마트 계약 조건이 오라클(외부 데이터 제공자)로부터 충분한 입찰이 이루어질 경우, 서비스 계약은 시작된다. 이때 오라클들을 제공하는 데이터의 정확도와 신뢰성을 기반으로 평가한다. 2) 둘째, 오라클링(Oracling)이다. 충분한 입찰을 통해 특정 매개변수에 대한 스마트 계약이 시작되면, 계약 이행을 위해 각 오라클들은 요청자에게 데이터를 제공한다. 3) 셋째, 집계(Aggregation)이다. 이는 특정 매개 변수 요청에 의하여 오라클들이 제출한 모든 데이터들은 평균화 및 가중치 계산되어 요청자에게 전달된다.	

블록체인 기술 종류 및 특징 비교

구분	BLOCKCHAIN	DAG	HASHGRAPH	HOLOCHAIN	TEMPO
개요	- 가장 인기있는 DLT 유형 중의 하나이며, 트랜잭션 레코드를 블록체인 장부에 보관하는 방식 - 암호화 기술을 적용한 연속적인 기록 목록으로 일종의 데이터베이스에 저장된 모든 종류의 디지털 정보를 의미	- DAG(Directed Acyclic Graph)은 방향성 비순환그래프로 기존 블록체인의 대안으로 블록 없는 분산원장 방식 - DAG 분산원장의 주요 장점 중 하나는 수수료 없는 나노 거래를 제공 할 수 있다는 점	- 블록체인이 없는 분산 원장으로 네트워크의 어떤 노드도 정보나 거래를 조작할 수 없음 - 동일한 타임 스탬프의 원장에 여러 트랜잭션이 병렬 구조로 저장되고, 원장의 모든 레코드를 "이벤트"라고 부름	- 블록 없는 분산원장으로 데이터 중심이 아닌 에이전트 중심이며, 모든 에이전트에 자체 포크 시스템을 제공 - 글로벌 합의 프로토콜을 사용하지 않고 개별 모듈을 사용하여 전체 원장 시스템을 형서	- 블록 없이 이벤트 순서로 원장에 추가되는 방식으로 타임 스탬프 기능을 제공하고 수정이 전혀 필요하지 않으므로 개인 및 공용 모듈에 사용 - 무거운 하드웨어 구성 요소가 필요하지 않아 모바일 장치에서도 작동
작동	- 다양한 노드가 트랜잭션이 들어 있는 블록을 형성하는데 채굴 또는 지분 방식으로 기여하고 그에 따른 보상으로 코인(토큰)을 지급하는 알고리즘	- 여러 개의 트랜잭션을 하나의 블록으로 묶지 않고, 개별 요소들끼리 상호 연결하여 거래하며, 루프를 생성하지 않고 무작위의 비순환구조로 합의	- 해시그래프 분산원장 시스템은 불특정 노드에게 Gossip 프로토콜을 사용하며, 주로 네트워크를 통한 거래에 관한 모든 종류의 정보를 중계	- 홀로체인은 네트워크상의 각 디바이스가 안전한 자체 원장 홀로체인을 갖고 독자적으로 작동하며, 다른 기기와 상호작용하는 탈 중앙화 솔루션	- 템포는 이벤트 시퀀스와 샤드방식을 채택하여 모든 노드는 전체 글로벌 원장의 하위 집합을 보유하도록 선택할 수 있어 확장성 향상
특성	- 불변성 : 변경, 삭제 불가능하고 원본 증명 - 보안 강화 : 분산구조 및 암호화로 해킹, 위변조거의 불가능 - 빠른 청산 : 기존 시스템보다 빠른 글로벌 결제 - 합의 지원 : 거래를 검증하기 위한 합의 알고리즘 사용	- 무한 확장성 : 자체 분산 원장 속성으로 무한 확장 - 마이크로 나노 거래 : 트랜잭션 단위로 미세 거래 가능 - 양자 저항 : 일회성 서명 체계로 양자 컴퓨터 등에 안전 - 병렬 거래 : 트랜잭션이 병렬방식으로 정렬	- 공정성 강화 : 노드가 동의하기 전에 거래 불가 - 고유한 데이터 구조 : 모든 가쉽시퀀스를 순서대로 기록 - 무작위 가쉽: 인접 노드로 무작위 선택 및 전달 - 가상 투표 : 가상 투표 시스템을 통해 빠른 합의 도달	- 에이전트 중심 : 강제 합의 없이 독립적 검증하고 스스로 관리 - 효율적 에너지 : 거래 검증이 가볍고 채굴 불필요 - 진정한 분산원장 : 자신의 장치에서 원장 실행 - 사용자 권한 : 모든 노드가 독립적으로 자신의 데이터를 제어	- 샤딩: 모든 노드는 고유 ID로 작은 로컬원장에 저장하고 유지 - 가쉽 프로토콜 : 모든 샤드 분산원장이 가쉽 방식으로 서로 빠르게 통신 - 논리 시계 : 트랜잭션에 타임 스탬프를 지정하는 대신 합의 도달을 위한 순서를 기억

블록체인 플랫폼 비교

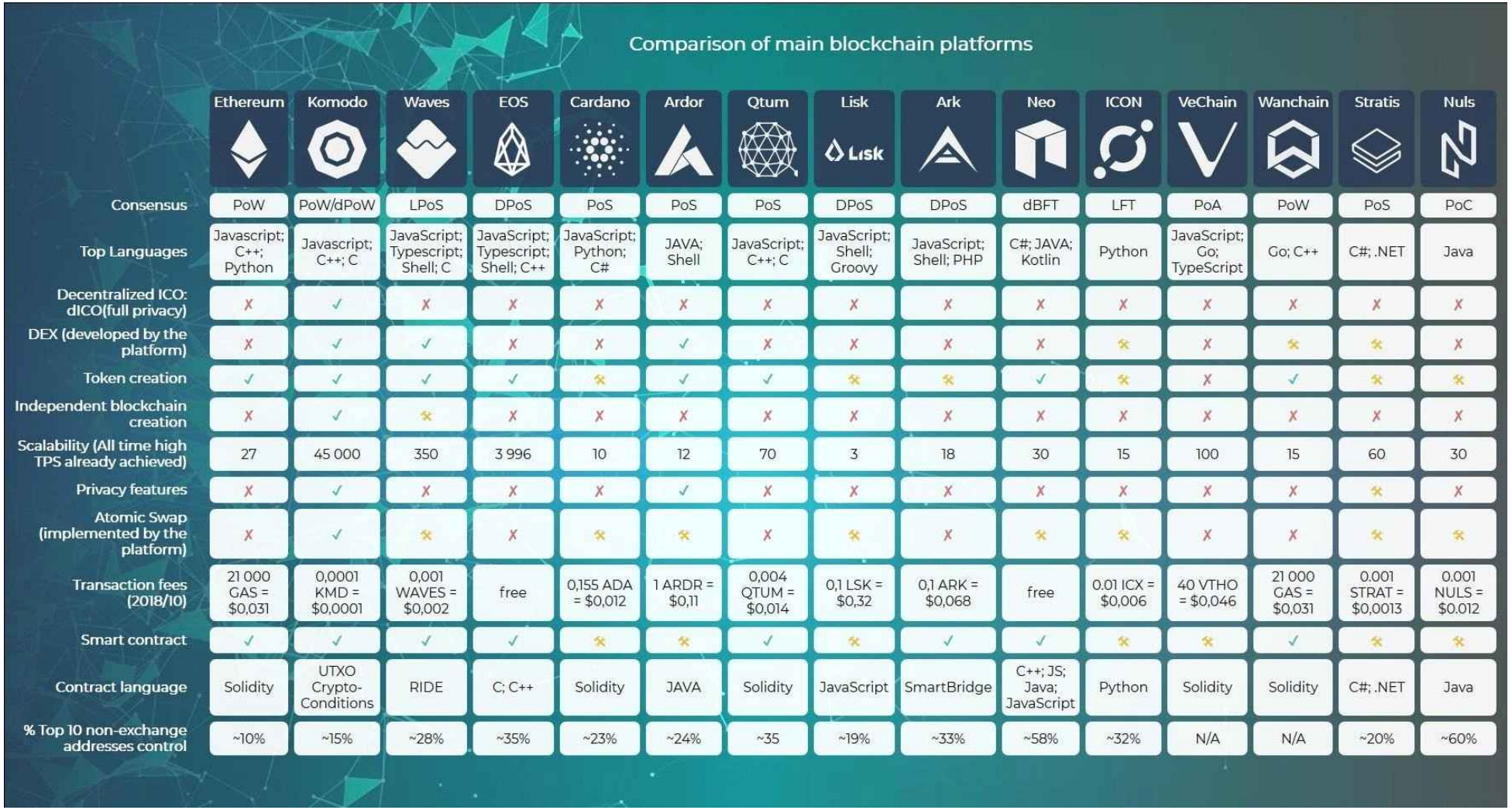
구분	Ethereum	Hyperledger	Quorum	Corda	Ripple
Development (Governance)	Ethereum Foundation	Linux Foundation	J. P. Morgan	R3	Ripple Labs
Service Type	Public Blockchain	Enterprise Blockchain	Enterprise Blockchain	Enterprise Blockchain	Payments Blockchain
Industry Focus	Cross-industry	Cross-industry	Cross-industry	Financial Services	Financial Services
Purpose (Preferred Usage)	B2C Business	B2C Business	Financial Services Industry	Financial Services Industry	Bankings and Financial Institutions
Smart Contracts Language	Solidity	Go, Java	Solidity	Kotlin, Java	C++
Currency	Ether(ETH)	Can be built using chaincodes	Ether(ETH)	No native cryptocurrency	Ripple(XRP)
Consensus	Proof of Work(PoW) used for decision marking	Not compulsory for all nodes to participate in consensus	Pluggable, Raft consensus, Istanbal BFT	Parties to a transation are involved in decision marking	Probabilistic Voting
Multi-tenancy	Not available	Supported using channels	Not available	Isolated and multi-tenant by design	Available
Throughput(tps)	15 ~ 25 tps	3,000 ~ 10,000 tps	A few 100s	170 tps	1,500 ~ 5,0000 tps

출처 : The 5 best blockchain platforms for enterprises and what makes them a good fit, 2019.1.4. 자료의 재편집

블록체인 플랫폼별 프로그래밍 언어

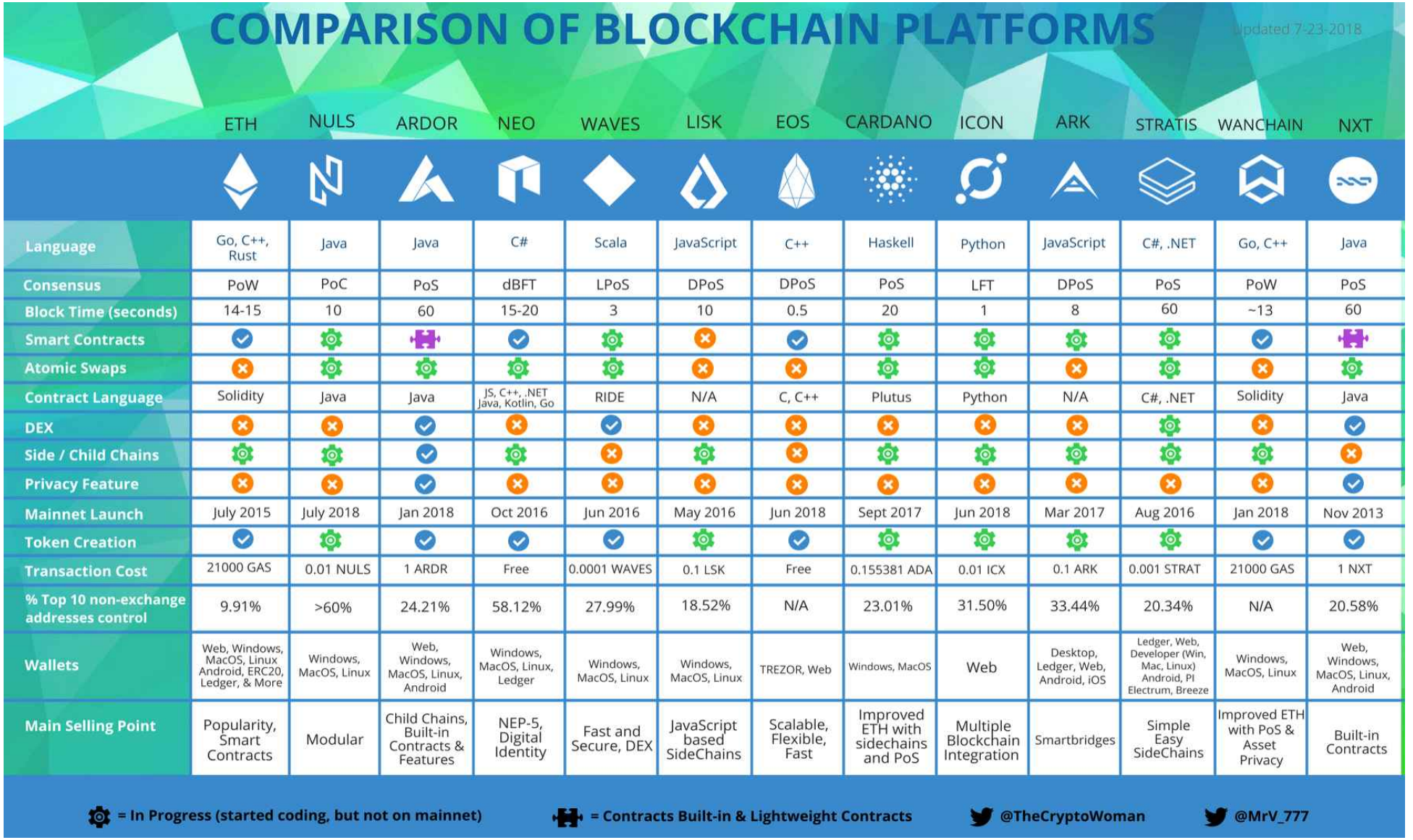
Blockchain Platform	Scripting Language	Open Source?	Main Implementation Languages	Software License
Bitcoin	Bitcoin Script[82,96]	Yes[185]	C++[185]	Bitcoin Core: MIT License[194]
Ethereum	Solidity (similar to C and Java Script), Serpent (similar to Python), and LLL (similar to Lisp)[103,182,183]	Yes[186–190]	Go-Ethereum: Go[186] CPP-Ethereum: C++[187] Py-Ethereum: Python[188] EthereumJ: Java[189] Parity: Rust[190]	Go-Ethereum: Lesser General Public License (LGPL) v3.0[186] CPP-Ethereum: General Public License (GPL) v3.0[187] Py-Ethereum: MIT License[188] EthereumJ: General Public License (GPL) v3.0[189] Parity: General Public License (GPL) v3.0[190]
Zcash	Bitcoin Script[125,150,176]	Yes[107]	C++[107]	Copyright by the Zcash developers and the Bitcoin Core developers[107]
Litecoin	Bitcoin Script[177]	Yes[191]	C++[191]	MIT License[191]
Dash	Bitcoin Script[82,178]	Yes[192]	C++[192]	MIT License[192]
Peercoin	Bitcoin Script[179,180]	Yes[193]	C++[193]	MIT License[193]
Ripple	N/A (Java Script for Codius, abandoned)[111,152,181]	Yes[84]	C++[84]	Various Copyrights[84]
Monero	N/A [GitHub](although the CryptoNote white paper states one[89])	Yes[195]	C++[195]	Copyright by The Monero Project[195]
MultiChain	Bitcoin Script[182,183]	Yes[113]	C++[113]	General Public License (GPL) v3.0 [113]
Hyperledger	Various, for example, Go/node.js for Fabric (Chaincode)[98], C++, Go, Java, JavaScript, Python, Rust, or Solidity (through Seth) for Sawtooth[154,184]	Yes[114]	Various, for example, Go for Fabric, Python for Sawtooth[114]	Various, for example, Apache License v2.0 for Fabric, Copyright by Intel Corporation for Sawtooth[114]

출처 : Tsung-Ting Kuo, Hugo Zavaleta Rojas, and Lucila Ohno-Machado, Comparison of blockchain platforms: a systematic review and healthcare examples, Journal of the American Medical Informatics Association, 26(5), 2019.3.25, pp.462-478.



	Ethereum	Komodo	Waves	EOS	Cardano	Ardor	Qtum	Lisk	Ark	Neo	ICON	VeChain	Wanchain	Stratis	Nuls
Consensus	PoW	PoW/dPoW	LPoS	DPoS	PoS	PoS	PoS	DPoS	DPoS	dBFT	LFT	PoA	PoW	PoS	PoC
Top Languages	Javascript; C++; Python	Javascript; C++; C	JavaScript; Typescript; Shell; C	JavaScript; Typescript; Shell; C++	JavaScript; Python; C#	JAVA; Shell	JavaScript; C++; C	JavaScript; Shell; Groovy	JavaScript; Shell; PHP	C#; JAVA; Kotlin	Python	JavaScript; Go; TypeScript	Go; C++	C#; .NET	Java
Decentralized ICO: dICO(full privacy)	✗	✓	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
DEX (developed by the platform)	✗	✓	✓	✗	✗	✓	✗	✗	✗	✗	⚒	✗	⚒	⚒	✗
Token creation	✓	✓	✓	✓	⚒	✓	✓	⚒	⚒	✓	⚒	✗	✓	⚒	⚒
Independent blockchain creation	✗	✓	⚒	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗	✗
Scalability (All time high TPS already achieved)	27	45 000	350	3 996	10	12	70	3	18	30	15	100	15	60	30
Privacy features	✗	✓	✗	✗	✗	✓	✗	✗	✗	✗	✗	✗	✗	⚒	✗
Atomic Swap (implemented by the platform)	✗	✓	⚒	✗	⚒	⚒	✗	⚒	✗	⚒	⚒	✗	✗	⚒	⚒
Transaction fees (2018/10)	21 000 GAS = $0,031	0,0001 KMD = $0,0001	0,001 WAVES = $0,002	free	0,155 ADA = $0,012	1 ARDR = $0,11	0,004 QTUM = $0,014	0,1 LSK = $0,32	0,1 ARK = $0,068	free	0.01 ICX = $0,006	40 VTHO = $0,046	21 000 GAS = $0,031	0.001 STRAT = $0,0013	0.001 NULS = $0.012
Smart contract	✓	✓	✓	✓	⚒	⚒	✓	⚒	✓	✓	⚒	⚒	✓	⚒	⚒
Contract language	Solidity	UTXO Crypto-Conditions	RIDE	C; C++	Solidity	JAVA	Solidity	JavaScript	SmartBridge	C++; JS; Java; JavaScript	Python	Solidity	Solidity	C#; .NET	Java
% Top 10 non-exchange addresses control	~10%	~15%	~28%	~35%	~23%	~24%	~35	~19%	~33%	~58%	~32%	N/A	N/A	~20%	~60%

출처 : www.reddit.com/r/komodoplatform/comments/9p87pv/new_platforms_comparison/, 2018.10.18

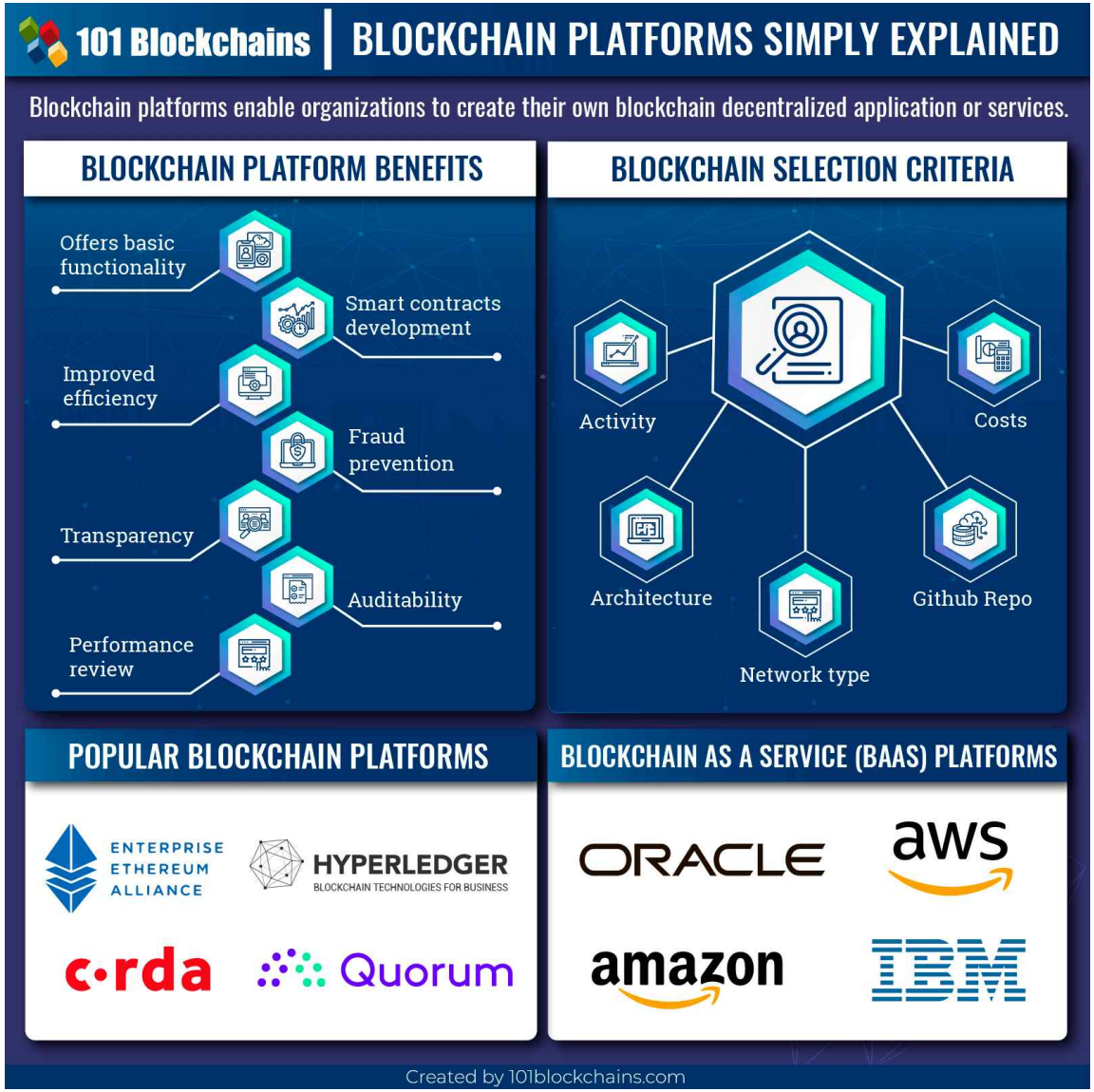


출처 : twitter.com/thecryptowoman/status/1021385599088054273, 2018.7.23.

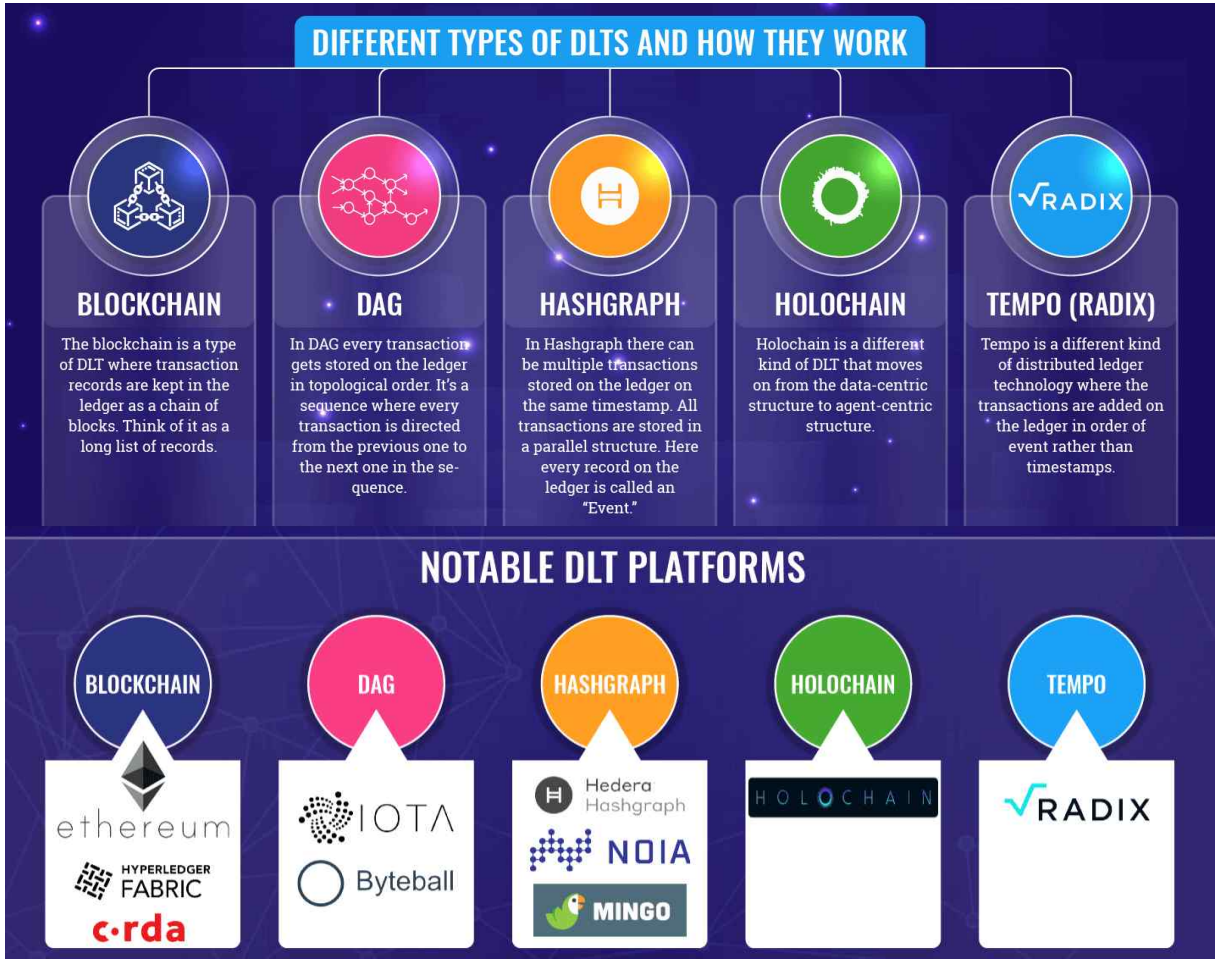
Table 2: Comparison of blockchain platforms

	Application	**Smart contract execution**	**Smart contract language**	**Data model**	**Consensus**
Hyperledger	Smart contract	Dockers	Golang, Java	Account-based	PBFT
Ethereum	Smart contract, Crypto-currency	EVM	Solidity, Serpent, LLL	Account-based	Ethash (PoW)
Eris-DB	Smart contract	EVM	Solidity	Account-based	Tendermint (BFT)
Ripple	Crypto-currency	-	-	UTXO-based	Ripple Consensus Ledger (PoS)
ScalableBFT	Smart contract	Haskell Execution	Pact	Account-based	ScalableBFT
Stellar	Smart contract	Dockers	JavaScript, Golang, Java, Ruby, Python, C#	Account-based	Stellar Consensus Protocol
Dfinity	Smart contract	EVM	Solidity, Serpent, LLL	Account-based	Blockchain Nervous System
Parity	Smart contract	EVM	Solidity, Serpent, LLL	Account-based	Proof of Authority
Tezos	Smart contract, Crypto-currency	Dockers	Tezos Contract Script Language	Account-based	Proof of Stake
Corda	Smart contract	JVM	Kotlin, Java	UTXO-based	Raft
Sawtooth Lake	Smart contract	TEE	Python	Account-based	Proof of Elapsed Time

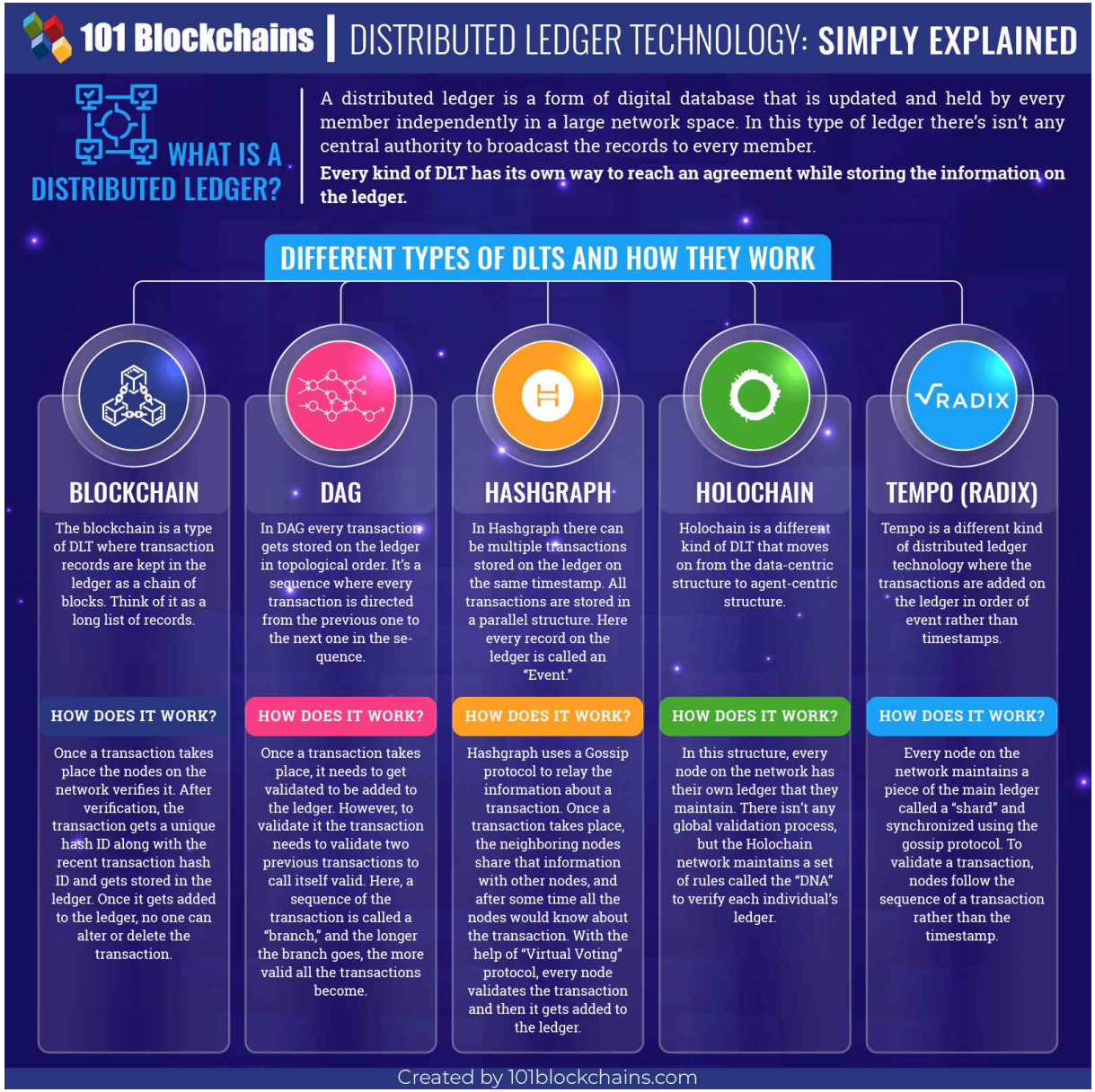
출처 : Tien Tuan Anh Dinh et al, BLOCKBENCH: A Framework for Analyzing Private Blockchains. 2017.3.12.

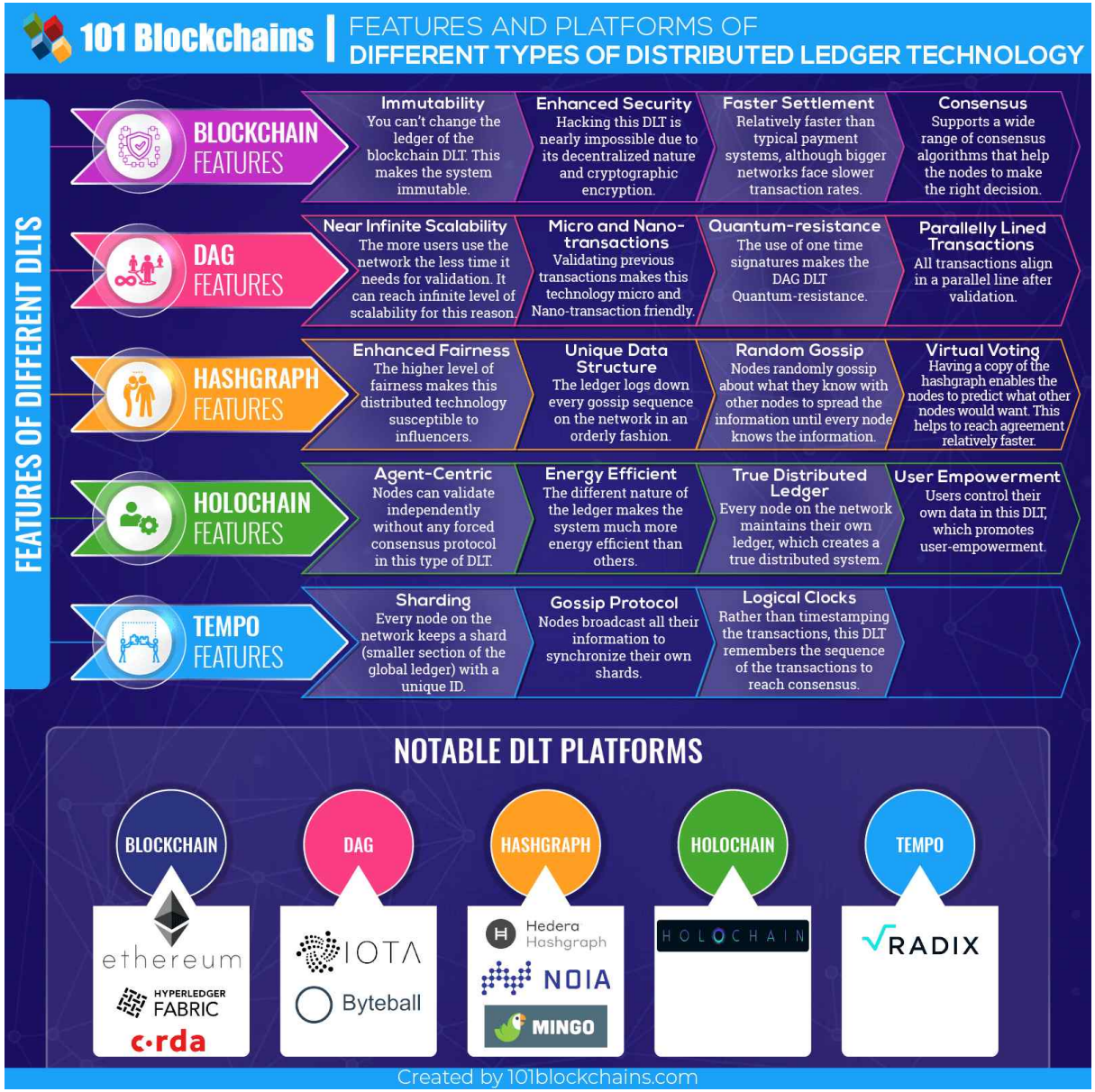


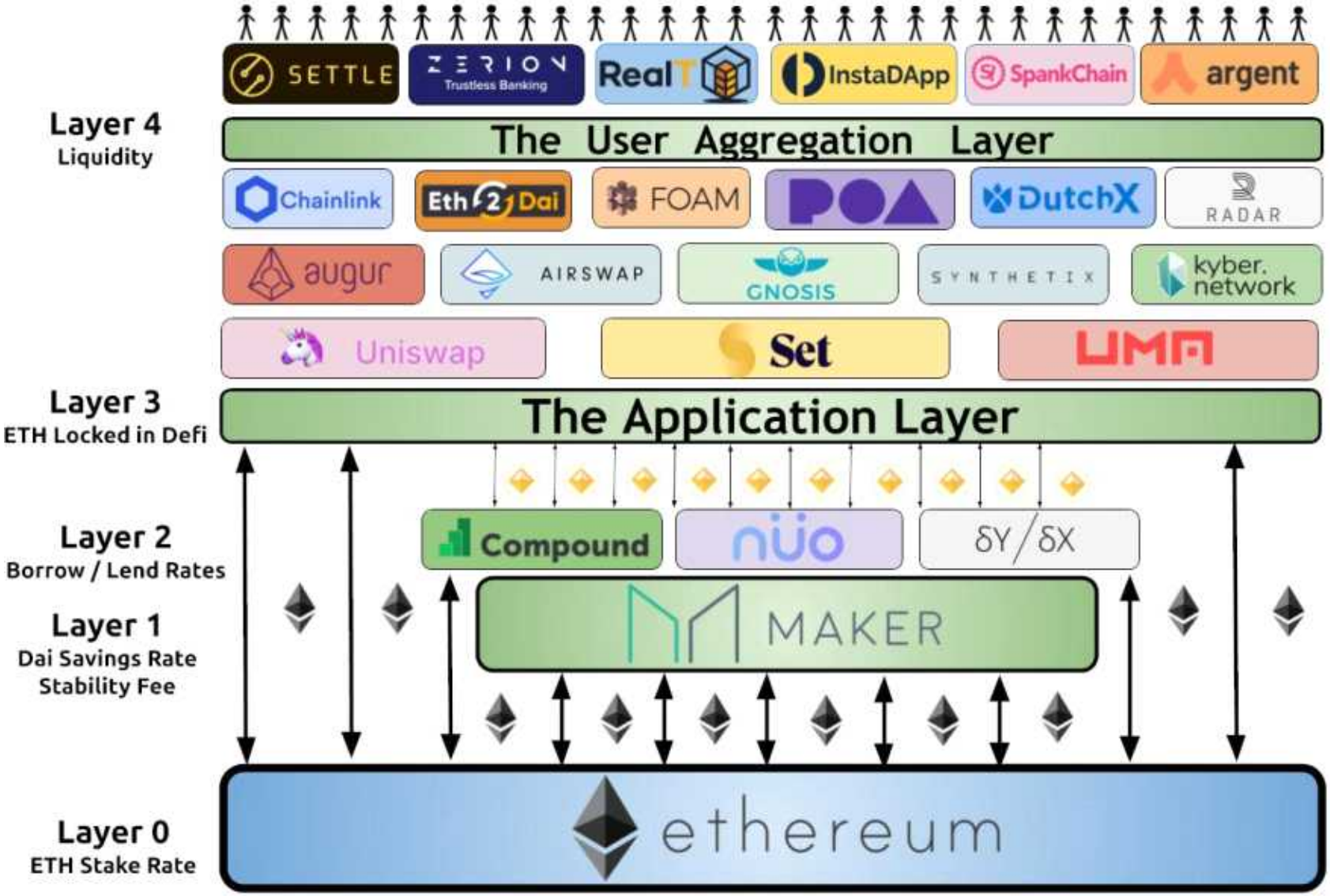
출처 : Top Blockchain Platforms and Enterprise Solutions to Choose From, 2019.7.29



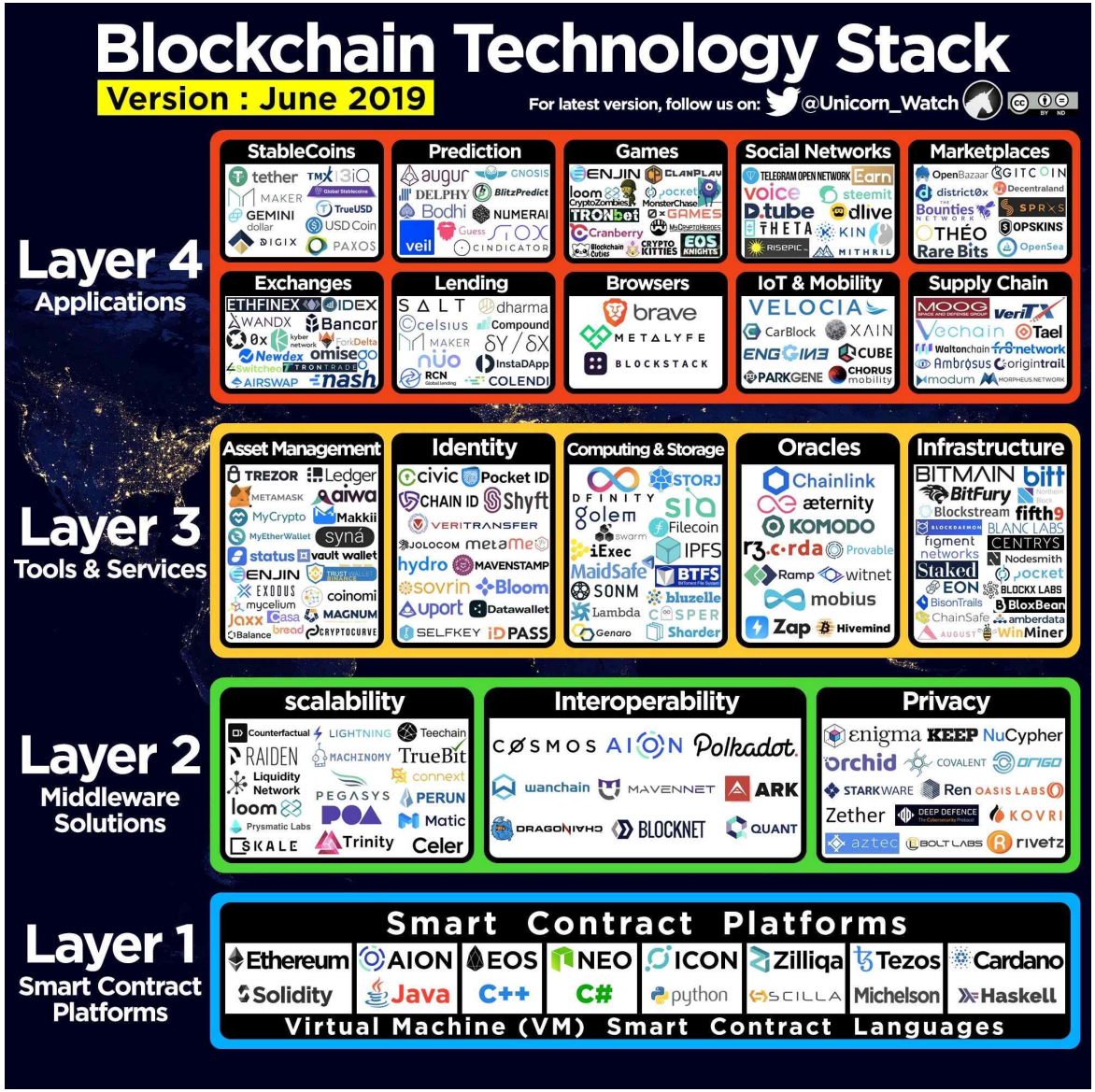
출처 : Distributed Ledger Technology: Where Technological Revolution Starts, 2019.1.30.


101 Blockchains | DISTRIBUTED LEDGER TECHNOLOGY: SIMPLY EXPLAINED
WHAT IS A DISTRIBUTED LEDGER?
A distributed ledger is a form of digital database that is updated and held by every member independently in a large network space. In this type of ledger there's isn't any central authority to broadcast the records to every member.
Every kind of DLT has its own way to reach an agreement while storing the information on the ledger.
DIFFERENT TYPES OF DLTS AND HOW THEY WORK
BLOCKCHAIN
The blockchain is a type of DLT where transaction records are kept in the ledger as a chain of blocks. Think of it as a long list of records.
HOW DOES IT WORK?
Once a transaction takes place the nodes on the network verifies it. After verification, the transaction gets a unique hash ID along with the recent transaction hash ID and gets stored in the ledger. Once it gets added to the ledger, no one can alter or delete the transaction.
DAG
In DAG every transaction gets stored on the ledger in topological order. It's a sequence where every transaction is directed from the previous one to the next one in the sequence.
HOW DOES IT WORK?
Once a transaction takes place, it needs to get validated to be added to the ledger. However, to validate it the transaction needs to validate two previous transactions to call itself valid. Here, a sequence of the transaction is called a "branch," and the longer the branch goes, the more valid all the transactions become.
HASHGRAPH
In Hashgraph there can be multiple transactions stored on the ledger on the same timestamp. All transactions are stored in a parallel structure. Here every record on the ledger is called an "Event."
HOW DOES IT WORK?
Hashgraph uses a Gossip protocol to relay the information about a transaction. Once a transaction takes place, the neighboring nodes share that information with other nodes, and after some time all the nodes would know about the transaction. With the help of "Virtual Voting" protocol, every node validates the transaction and then it gets added to the ledger.
HOLOCHAIN
Holochain is a different kind of DLT that moves on from the data-centric structure to agent-centric structure.
HOW DOES IT WORK?
In this structure, every node on the network has their own ledger that they maintain. There isn't any global validation process, but the Holochain network maintains a set of rules called the "DNA" to verify each individual's ledger.
TEMPO (RADIX)
Tempo is a different kind of distributed ledger technology where the transactions are added on the ledger in order of event rather than timestamps.
HOW DOES IT WORK?
Every node on the network maintains a piece of the main ledger called a "shard" and synchronized using the gossip protocol. To validate a transaction, nodes follow the sequence of a transaction rather than the timestamp.
Created by 101blockchains.com


101 Blockchains
FEATURES AND PLATFORMS OF
DIFFERENT TYPES OF DISTRIBUTED LEDGER TECHNOLOGY
FEATURES OF DIFFERENT DLTS
BLOCKCHAIN FEATURES
Immutability
You can't change the ledger of the blockchain DLT. This makes the system immutable.
Enhanced Security
Hacking this DLT is nearly impossible due to its decentralized nature and cryptographic encryption.
Faster Settlement
Relatively faster than typical payment systems, although bigger networks face slower transaction rates.
Consensus
Supports a wide range of consensus algorithms that help the nodes to make the right decision.
DAG FEATURES
Near Infinite Scalability
The more users use the network the less time it needs for validation. It can reach infinite level of scalability for this reason.
Micro and Nano-transactions
Validating previous transactions makes this technology micro and Nano-transaction friendly.
Quantum-resistance
The use of one time signatures makes the DAG DLT Quantum-resistance.
Parallelly Lined Transactions
All transactions align in a parallel line after validation.
HASHGRAPH FEATURES
Enhanced Fairness
The higher level of fairness makes this distributed technology susceptible to influencers.
Unique Data Structure
The ledger logs down every gossip sequence on the network in an orderly fashion.
Random Gossip
Nodes randomly gossip about what they know with other nodes to spread the information until every node knows the information.
Virtual Voting
Having a copy of the hashgraph enables the nodes to predict what other nodes would want. This helps to reach agreement relatively faster.
HOLOCHAIN FEATURES
Agent-Centric
Nodes can validate independently without any forced consensus protocol in this type of DLT.
Energy Efficient
The different nature of the ledger makes the system much more energy efficient than others.
True Distributed Ledger
Every node on the network maintains their own ledger, which creates a true distributed system.
User Empowerment
Users control their own data in this DLT, which promotes user-empowerment.
TEMPO FEATURES
Sharding
Every node on the network keeps a shard (smaller section of the global ledger) with a unique ID.
Gossip Protocol
Nodes broadcast all their information to synchronize their own shards.
Logical Clocks
Rather than timestamping the transactions, this DLT remembers the sequence of the transactions to reach consensus.
NOTABLE DLT PLATFORMS
BLOCKCHAIN
ethereum
HYPERLEDGER FABRIC
corda
DAG
IOTA
Byteball
HASHGRAPH
Hedera Hashgraph
NOIA
MINGO
HOLOCHAIN
HOLOCHAIN
TEMPO
RADIX
Created by 101blockchains.com



출처 : DavidHoffman.eth, TrustlessState, Aug 14, 2019.



출처 : Unicorn Watch, Mapping out the Blockchain Technology Stack, June 16, 2019.

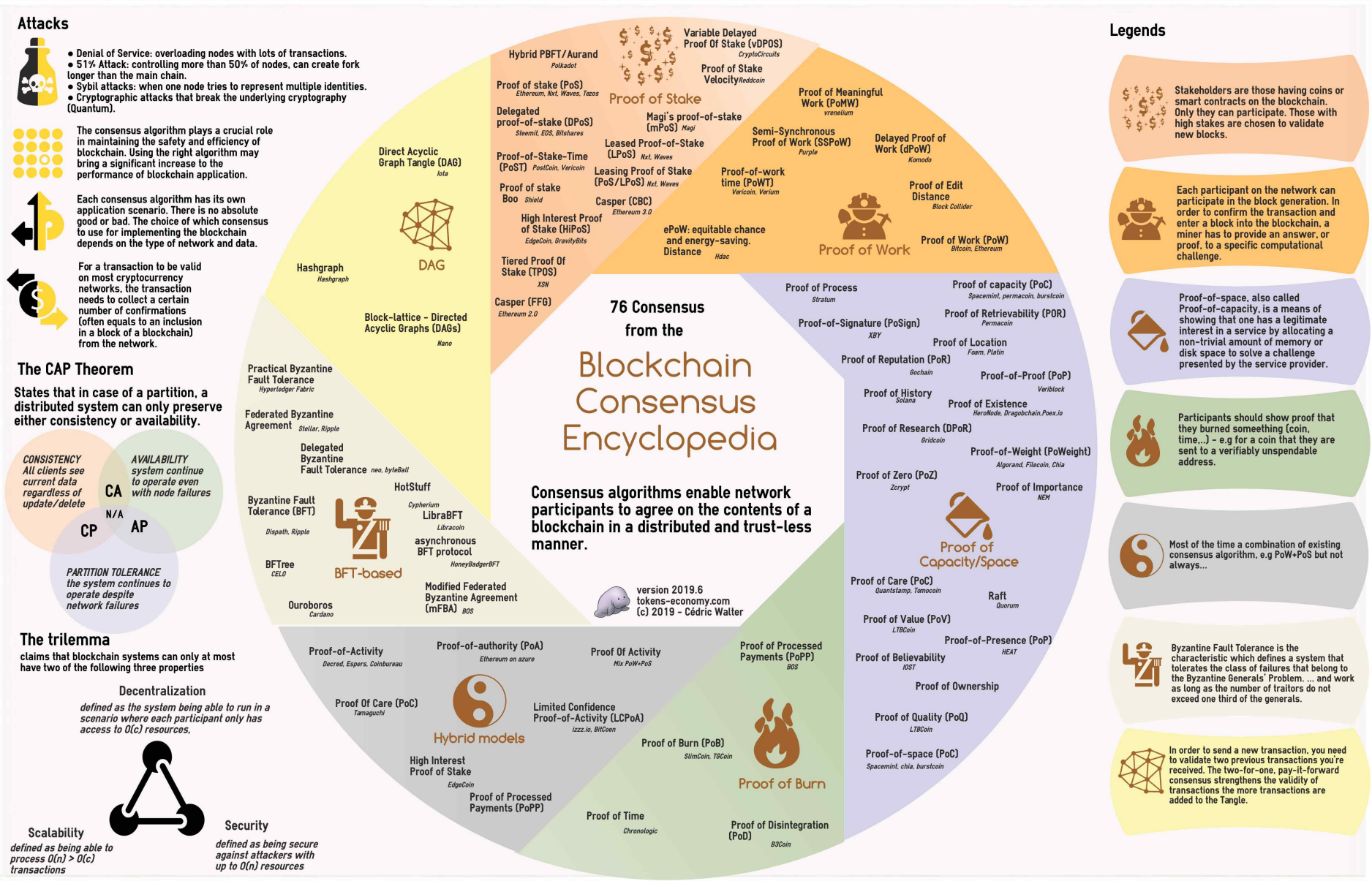
Comparison of consensus algorithms based on their representative cryptocurrencies(coincheckup, 2019).

Row	Consensus algorithms	Cryptocurrencies	Algorithm	Genesis Block	Rank	Market CAP ($)	TPS	Block Time Minutes	Mining reward
1	PoW	Bitcoin	SHA256	January 3, 2009	1	180,207,092,238	7	10	12.5 BTC
		Ethereum	Ethash (KECCAK256	July 30, 2015	2	22,757,000,420	15	0.25	2
		Litecoin	Scrypt	October 8, 2011	5	4,587,952,794	28	2.3	25
		Monero	Cryptonight	April 18, 2014	11	1,268,871,523	30	2	4.9
		Zcash	Equihash	October 28, 2016	28	348,443,197	27	2	10
2	PoS	Waves (LPoS)	LPoS	June 12, 2016	55	100,304,755	100	1	Non-minebable
		Qtum	POS 3.0	December 26, 2016	36	202,601,750	70	2	Non-minebable
		Nxt	SHA256	November 24, 2013	175	16,162,355	100	1	Non-minebable
		Blackcoin	Scrypt	February 24, 2014	500	4,569,548	0	1	Non-minebable
		Nano	Blake2b	February 29, 2016	45	123,741,646	7000	Instant	Non-minebable
3	DPoS	EOS	DPoS	July 1, 2017	7	3,641,735,649	4000	0.5	Non-minebable
		Cardano	Ouroboros (DPoS)	December 26, 2017	12	1,266,573,741	257	0.33	Non-minebable
		TRON	DPoS	August 28, 2017	13	1,186,299,015	2000	0.05	32 TRON
		Lisk	DPoS	January 30, 2016	47	118,714,644	3	0.284	Non-minebable
		BitShares	DPoS	July 19, 2014	58	91,575,735	100000	0.05	Non-minebable
4	PBFT	Ripple	N/A	April 11, 2013	3	12,010,477,031	1500	0.06	Non-minebable
		Stellar	N/A	April 6, 2016	10	1,410,189,643	1000	0.08	Non-minebable
		Zilliqa	Keccak	January 12, 2018	79	59,022,911	0	45s to 4 m	Non-minebable
5	PoC	Burst	Shabal256	August 11, 2014	190	14,417,212	80	4	460
6	DAG	IOTA	Curl-P	October 21, 2015	17	788,711,735	1000	Instant	Non-minebable
		Byteball (Obyte)	DAG	September 5, 2016	262	17,301,594	10	0.5	Non-minebable
		Travelflex	DAG	December 2, 2017	1374	163,648	3500	1	30.00 TRF
7	PoA (Hybrid PoW/PoS)	Dash	X11	January 19, 2014	16	850,165,302	56	2.5	2.09
		Decred	BLAKE256	December 15, 2015	32	233,089,579	14	5	18.22
		Komodo	Equihash	September 1, 2016	67	80,699,867	100	1	3.00 KMD
		Peercoin	SHA-256	August 19, 2012	373	7,844,163	0	10	37.36 PPC
		Espers	HMQ1725	April 28, 2016	1026	625,199	0	5	5000
8	dBFT	NEO	RIPEMD160	October 17, 2016	20	650,866,809	1000	0.25	Non-minebable
9	PoI	NEM (XEM)	Ed25519	March 31, 2015	26	403,570,701	10000	1	Non-minebable
10	PoB	Slimcoin	Dcrypt	May 07 2014	2661	16,195	0.00003	1.5	50.00 SLM

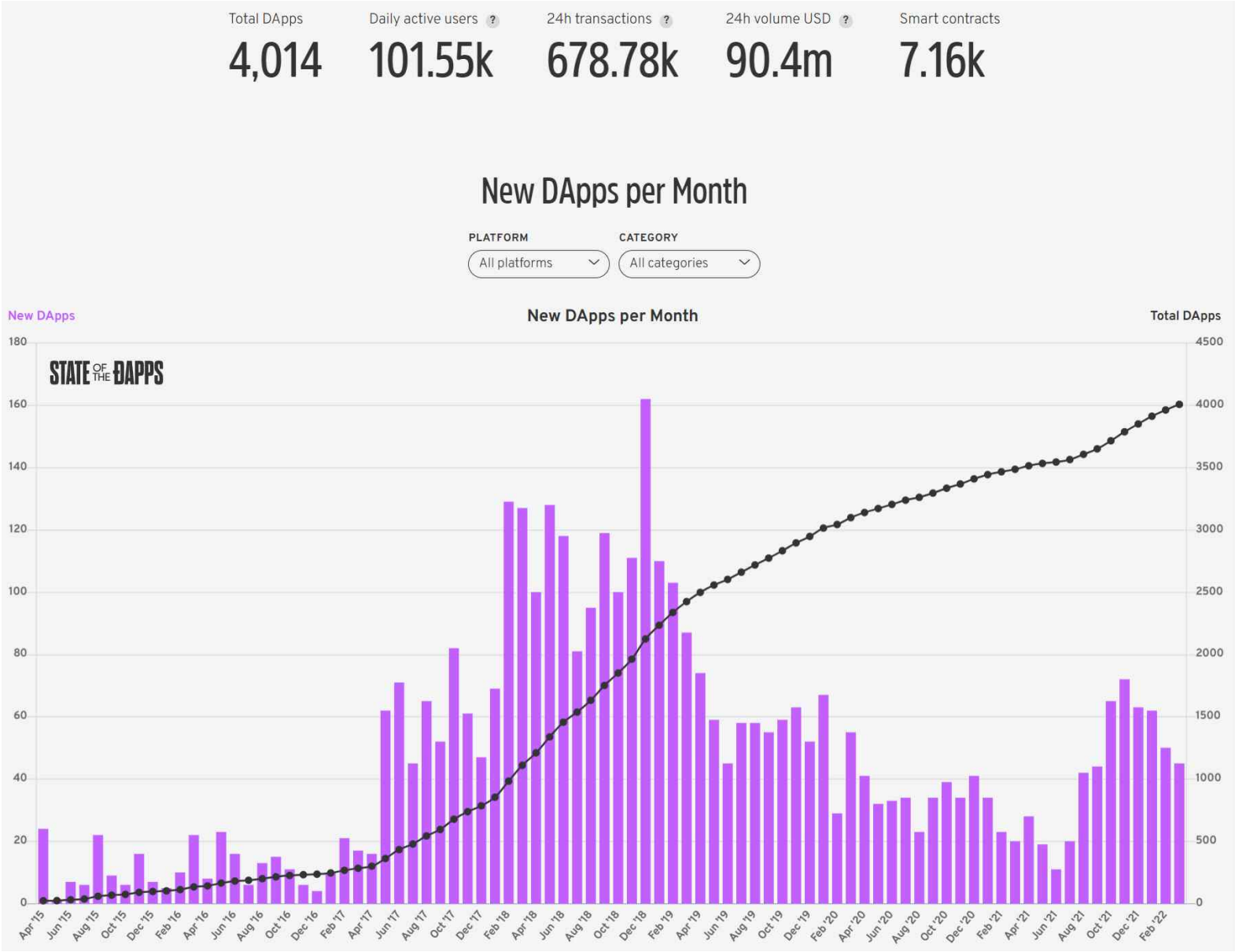
Summary comparison of blockchain consensus algorithms

Consensus algorithms	Designing Goal	Decentralization level	Permission model/ Node Identity Management	Electing Miners/ verifiers Based on	Energy efficiency	Scalability	%51 Attack	Double Spendingattack	Hardware dependency	speed
PoW	Sybil-proof	Decentralized	Permissionless	Work (Hash)	No	Strong	Vulnerable	Vulnerable	Yes	Slow
PoS	Energy efficiency	Semi-centralized	Permissionless	Stake	Yes	Strong	Vulnerable	Difficult	No	Fast
DPoS	Organize PoS effectively	Semi-centralized	Both	Vote	Yes	Strong	Vulnerable	Vulnerable	No	Fast
PBFT	Remove software errors	Decentralized	Both	Vote	Yes	Low	Safe	Safe	No	Slow
PoC	Less energy than PoW	Decentralized	Permissionless	Work (Hash)	Fair	Strong	Vulnerable	Vulnerable	Yes	Slow
DAG	Speed and Scalability	Decentralized	Permissionless	N/A	Yes	Strong	Safe	Safe	No	Fast
PoA	Benefits of both Pos and PoW	Decentralized	Permissioned	Vote and work	No	Strong	Safe	Vulnerable	Yes	Fair
dBFT	Faster PBFT	Semi-centralized	Permissioned	Vote	Yes	Medium	Vulnerable	Vulnerable	No	Slow
PoI	Improve PoS	Decentralized	Permissionless	Importance scores	Yes	Strong	Safe	Safe	No	Fast
PoB	N/A	Decentralized	Permissionless	Burnt coins	No	Medium	Vulnerable	vulnerable	No	Fast

출처: A survey of blockchain consensus algorithms performance evaluation criteria, Expert Systems With Application, 2020.9.15.

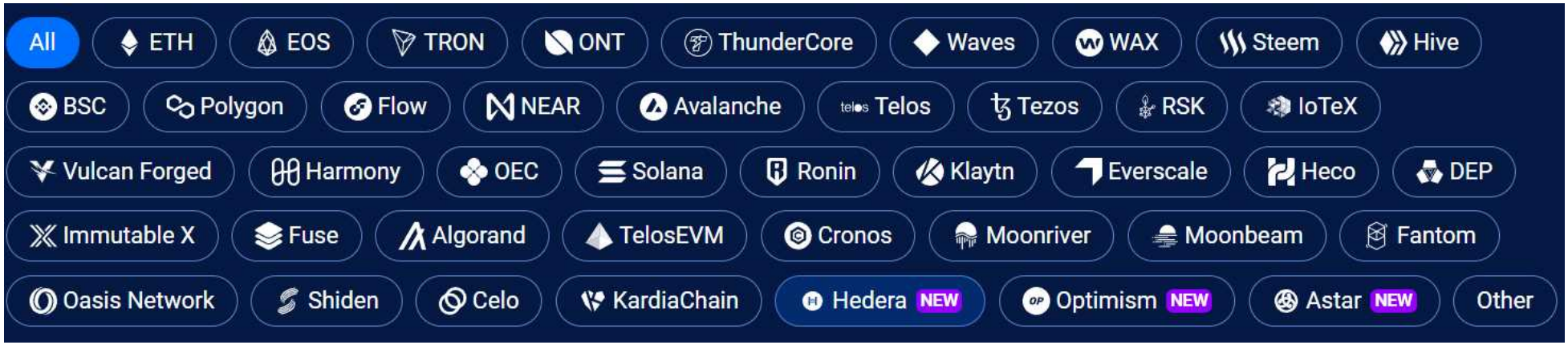

Attacks
• Denial of Service: overloading nodes with lots of transactions.
• 51% Attack: controlling more than 50% of nodes, can create fork longer than the main chain.
• Sybil attacks: when one node tries to represent multiple identities.
• Cryptographic attacks that break the underlying cryptography (Quantum).
The consensus algorithm plays a crucial role in maintaining the safety and efficiency of blockchain. Using the right algorithm may bring a significant increase to the performance of blockchain application.
Each consensus algorithm has its own application scenario. There is no absolute good or bad. The choice of which consensus to use for implementing the blockchain depends on the type of network and data.
For a transaction to be valid on most cryptocurrency networks, the transaction needs to collect a certain number of confirmations (often equals to an inclusion in a block of a blockchain) from the network.
The CAP Theorem
States that in case of a partition, a distributed system can only preserve either consistency or availability.
CONSISTENCY All clients see current data regardless of update/delete
AVAILABILITY system continue to operate even with node failures
PARTITION TOLERANCE the system continues to operate despite network failures
CA
CP
AP
N/A
The trilemma
claims that blockchain systems can only at most have two of the following three properties
Decentralization
defined as the system being able to run in a scenario where each participant only has access to O(c) resources,
Scalability
defined as being able to process O(n) > O(c) transactions
Security
defined as being secure against attackers with up to O(n) resources
76 Consensus from the
Blockchain Consensus Encyclopedia
Consensus algorithms enable network participants to agree on the contents of a blockchain in a distributed and trust-less manner.
version 2019.6
tokens-economy.com
(c) 2019 - Cédric Walter
Proof of Stake
Variable Delayed Proof Of Stake (vDPOS) CryptoCircuits
Proof of Stake Velocity Reddcoin
Hybrid PBFT/Aurand Polkadot
Proof of stake (PoS) Ethereum, Nxt, Waves, Tezos
Delegated proof-of-stake (DPoS) Steemit, EOS, Bitshares
Magi's proof-of-stake (mPoS) Magi
Leased Proof-of-Stake (LPoS) Nxt, Waves
Proof-of-Stake-Time (PoST) PostCoin, Vericoin
Leasing Proof of Stake (PoS/LPoS) Nxt, Waves
Proof of stake Boo Shield
Casper (CBC) Ethereum 3.0
High Interest Proof of Stake (HiPoS) EdgeCoin, GravityBits
Tiered Proof Of Stake (TPOS) XSN
Casper (FFG) Ethereum 2.0
Proof of Work
Proof of Meaningful Work (PoMW) vrenelium
Semi-Synchronous Proof of Work (SSPoW) Purple
Delayed Proof of Work (dPoW) Komodo
Proof-of-work time (PoWT) Vericoin, Verium
Proof of Edit Distance Block Collider
ePoW: equitable chance and energy-saving. Distance Hdac
Proof of Work (PoW) Bitcoin, Ethereum
DAG
Direct Acyclic Graph Tangle (DAG) Iota
Hashgraph Hashgraph
Block-lattice - Directed Acyclic Graphs (DAGs) Nano
BFT-based
Practical Byzantine Fault Tolerance Hyperledger Fabric
Federated Byzantine Agreement Stellar, Ripple
Delegated Byzantine Fault Tolerance neo, byteBall
HotStuff Cypherium
Byzantine Fault Tolerance (BFT) Dispath, Ripple
LibraBFT Libracoin
asynchronous BFT protocol HoneyBadgerBFT
BFTree CELO
Modified Federated Byzantine Agreement (mFBA) BOS
Ouroboros Cardano
Proof of Capacity/Space
Proof of Process Stratum
Proof of capacity (PoC) Spacemint, permacoin, burstcoin
Proof of Retrievability (POR) Permacoin
Proof-of-Signature (PoSign) XBY
Proof of Location Foam, Platin
Proof of Reputation (PoR) Gochain
Proof-of-Proof (PoP) Veriblock
Proof of History Solana
Proof of Existence HeroNode, Dragobchain,Poex.io
Proof of Research (DPoR) Gridcoin
Proof-of-Weight (PoWeight) Algorand, Filecoin, Chia
Proof of Zero (PoZ) Zcrypt
Proof of Importance NEM
Proof of Care (PoC) Quantstamp, Tomocoin
Raft Quorum
Proof of Value (PoV) LTBCoin
Proof-of-Presence (PoP) HEAT
Proof of Believability IOST
Proof of Ownership
Proof of Quality (PoQ) LTBCoin
Proof-of-space (PoC) Spacemint, chia, burstcoin
Hybrid models
Proof-of-Activity Decred, Espers, Coinbureau
Proof-of-authority (PoA) Ethereum on azure
Proof Of Activity Mix PoW+PoS
Proof Of Care (PoC) Tamaguchi
Limited Confidence Proof-of-Activity (LCPoA) izzz.io, BitCoen
High Interest Proof of Stake EdgeCoin
Proof of Processed Payments (PoPP)
Proof of Burn
Proof of Processed Payments (PoPP) BOS
Proof of Burn (PoB) SlimCoin, TGCoin
Proof of Time Chronologic
Proof of Disintegration (PoD) B3Coin
Legends
Stakeholders are those having coins or smart contracts on the blockchain. Only they can participate. Those with high stakes are chosen to validate new blocks.
Each participant on the network can participate in the block generation. In order to confirm the transaction and enter a block into the blockchain, a miner has to provide an answer, or proof, to a specific computational challenge.
Proof-of-space, also called Proof-of-capacity, is a means of showing that one has a legitimate interest in a service by allocating a non-trivial amount of memory or disk space to solve a challenge presented by the service provider.
Participants should show proof that they burned someething (coin, time,..) - e.g for a coin that they are sent to a verifiably unspendable address.
Most of the time a combination of existing consensus algorithm, e.g PoW+PoS but not always...
Byzantine Fault Tolerance is the characteristic which defines a system that tolerates the class of failures that belong to the Byzantine Generals' Problem. ... and work as long as the number of traitors do not exceed one third of the generals.
In order to send a new transaction, you need to validate two previous transactions you're received. The two-for-one, pay-it-forward consensus strengthens the validity of transactions the more transactions are added to the Tangle.

	VELAS	SOLANA	TRON	ethereum	EOS	neo
Transaction per second	up to 75000	up to 75000	2000	17	3996	1000
Average fee per transaction	$0.00001	$0.0025	free	$20.00	free	$0.60
Transaction latency	0.4 sec	0.4 sec	3 sec	5 min	2.5 min	15 sec
Number of validators	129	1272	27	200000	21	21
Total transactions to date	1.5 Billion	43 Billion	2.6 Billion	1.3 Billion	4.1 Billion	123 Million


Total DApps
4,014
Daily active users
101.55k
24h transactions
678.78k
24h volume USD
90.4m
Smart contracts
7.16k
New DApps per Month
PLATFORM
All platforms
CATEGORY
All categories
New DApps
New DApps per Month
Total DApps
STATE OF THE DAPPS
180
160
140
120
100
80
60
40
20
0
4500
4000
3500
3000
2500
2000
1500
1000
500
0
Apr '15
Jun '15
Aug '15
Oct '15
Dec '15
Feb '16
Apr '16
Jun '16
Aug '16
Oct '16
Dec '16
Feb '17
Apr '17
Jun '17
Aug '17
Oct '17
Dec '17
Feb '18
Apr '18
Jun '18
Aug '18
Oct '18
Dec '18
Feb '19
Apr '19
Jun '19
Aug '19
Oct '19
Dec '19
Feb '20
Apr '20
Jun '20
Aug '20
Oct '20
Dec '20
Feb '21
Apr '21
Jun '21
Aug '21
Oct '21
Dec '21
Feb '22

Platform	Total DApps	Daily active users	Transactions (24hr)	Volume (24hr)	# of contracts
Ethereum	2,948	51.06k	104.77k	29.66k	4.89k
EOS	332	45.59k	402.35k	124.75k	550
BSC	216	?	?	?	354
TRON	88	1.03k	3.9k	439.27k	281
Klaytn	81	?	?	?	316
Steem	79	?	?	?	177
Hive	56	?	?	?	105
Moonriver	38	?	?	?	82
Blockstack	24	?	?	?	0
Neo	24	?	?	?	30
NEAR	24	2.37k	157.74k	39	21
POA	21	1	5	0	51
xDai	21	15	193	136.65k	58
Obyte	17	17	359	131	162
ICON	16	1.47k	9.47k	5.95k	36
Loom	14	?	?	?	33
GoChain	7	?	?	?	17
Meter	6	?	?	?	0
OST	2	?	?	?	2

Top Blockchain Dapps



출처: https://dappradar.com/rankings, 2022.4.