

블록체인 메커니즘 및 플랫폼
(2 of 2)



- **블록체인 메커니즘**
- **블록체인 플랫폼**



블록체인 플랫폼

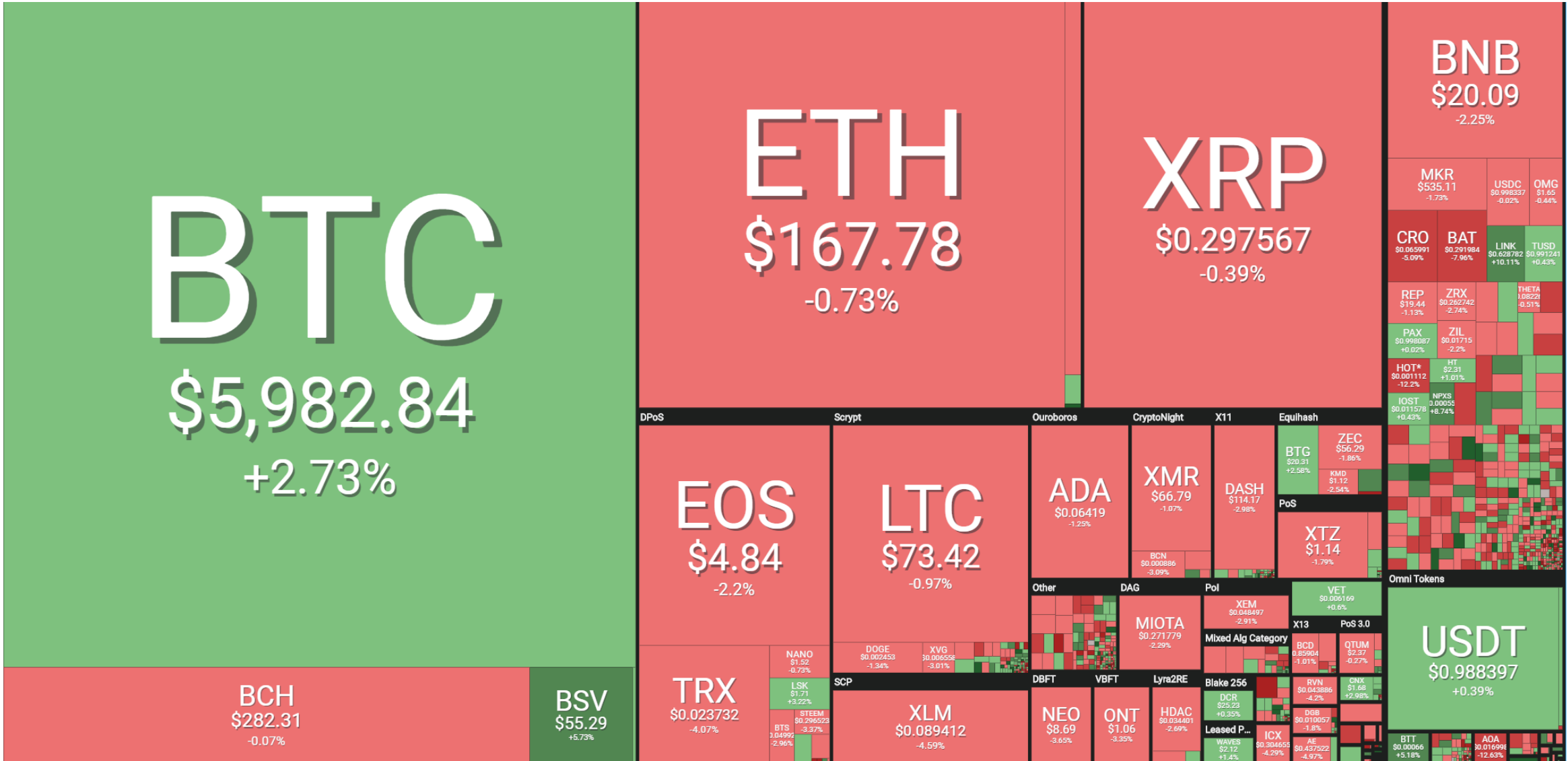
- 1세대 (2009~2014) - Bitcoin
 - 가상통화
 - 자산거래
- 2세대 (2015~현재) – Ethereum, Hyperledger
 - 스마트계약 (비즈니스 자동화)
 - 분산앱 (Decentralized Application)
- 3세대 (현재진행중) – 다양한 플랫폼들
 - Scalability
 - Interoperability
 - IoT support

2. 블록체인 플랫폼: CoinMarketCap (상위10개 코인)















암호화폐 ▾ 거래소 ▾ 관심 목록 KRW ▾ 다음 100 → 모두 보기

#	이름	시가총액	가격	거래량(24시간)	유통 공급량	변경(24시간)	가격 그래프(7일)
1	Bitcoin	₩126,985,748,766,723	₩7,178,026	₩19,181,139,410,835	17,690,900 BTC	2.54%	
2	Ethereum	₩21,259,251,114,288	₩200,567	₩7,873,319,653,976	105,995,979 ETH	-0.64%	
3	XRP	₩14,899,416,143,472	₩353.63	₩1,057,470,053,747	42,133,310,721 XRP *	-0.70%	
4	Bitcoin Cash	₩5,982,310,127,995	₩336,604	₩1,651,747,257,267	17,772,550 BCH	-0.39%	
5	Litecoin	₩5,379,863,056,298	₩87,200.73	₩3,143,165,479,970	61,695,157 LTC	-0.74%	
6	EOS	₩5,213,384,427,934	₩5,723.41	₩1,951,131,590,579	910,887,960 EOS *	-1.22%	
7	Binance Coin	₩3,384,144,883,156	₩23,971.19	₩206,884,369,240	141,175,490 BNB *	-1.76%	
8	Tether	₩3,294,477,822,005	₩1,186.52	₩15,916,018,375,270	2,776,595,295 USDT *	0.56%	
9	Stellar	₩2,058,815,510,601	₩107.44	₩247,161,446,283	19,162,820,780 XLM *	-3.78%	
10	Cardano	₩1,914,630,736,218	₩73.85	₩53,144,179,785	25,927,070,538 ADA	-3.53%	

2. 블록체인 플랫폼: Coin360 분류



2. 블록체인 플랫폼: CoinMarketCap (전체)

2151	 TOKOK	TOK	\$?	\$0.004427	? *	\$0	-0.47%	-0.35%	-6.59%	...
2152	 Gamblica	GMBC	\$?	\$0.000972	? *	\$0	0.00%	2.83%	11.04%	...
2153	 COZ	COZ	\$?	\$0.124183	? *	\$0	0.00%	0.00%	0.00%	...
2154	 UTEMIS	UTS	\$?	\$0.000272	? *	\$0	0.00%	-1.09%	4.01%	...
2155	 RabbitCoin	RBBT	\$?	\$0.000003	?	\$?	0.00%	0.00%	20.76%	...
2156	 Bubble	BUB	\$?	\$0.003023	? *	\$?	0.00%	0.00%	6.35%	...
2157	 Axiom	AXIOM	\$?	\$0.004442	?	\$?	0.00%	0.00%	0.00%	...
2158	 ClubCoin	CLUB	\$?	\$0.207019	? *	\$?	0.00%	0.00%	1.76%	...
2159	 AvatarCoin	AV	\$?	\$0.141351	? *	\$?	0.00%	0.00%	75.85%	...
2160	 Francs	FRN	\$?	\$0.003325	?	\$?	0.00%	0.00%	0.00%	...
2161	 Aces	ACES	\$?	\$0.000052	? *	\$?	0.00%	0.00%	0.00%	...
2162	 Wink	WINK	\$?	\$0.000106	? *	\$?	0.00%	0.00%	0.00%	...
2163	 Ethereum Lite	ELITE	\$?	\$0.079566	? *	\$?	0.00%	0.00%	0.00%	...
2164	 BTCMoon	BTCM	\$?	\$0.001719	? *	\$?	0.00%	0.00%	25.27%	...

* Not Mineable

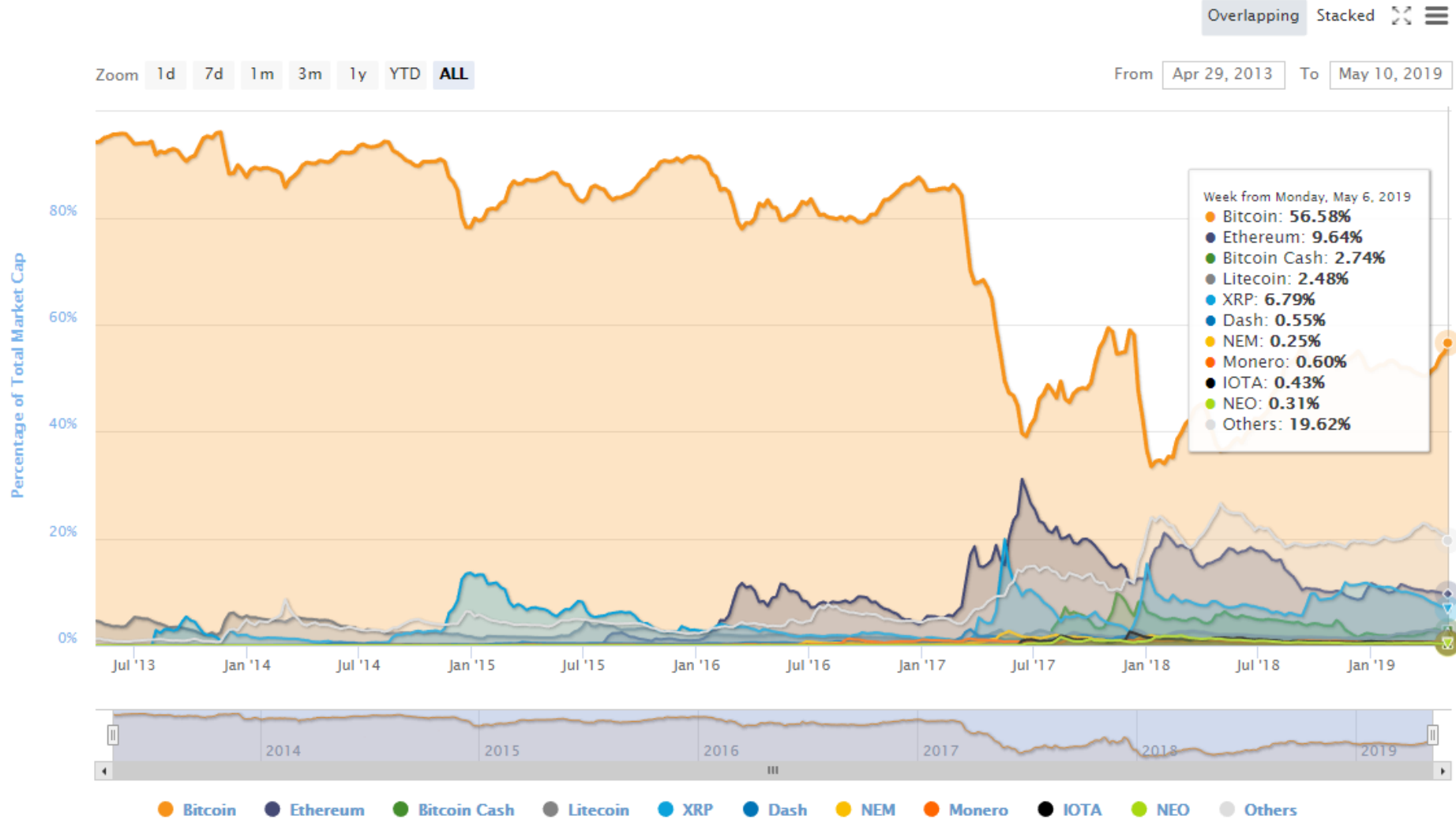
[← Back to Top 100](#)

Total Market Cap: \$187,142,041,881

Last updated: May 09, 2019 12:50 PM UTC

2. 블록체인 플랫폼: 전체코인시장

Percentage of Total Market Capitalization (Dominance)



Global Charts

Total Market Capitalization



2. 블록체인 플랫폼: 전체 코인 시장 가치(비트코인 제외)

10

Total Market Capitalization (Excluding Bitcoin)



- 해외 ICO

- Ethereum (2014.6) \$18M모금
- FileCoin \$257M 모금 (2017.8)

- 한국 ICO

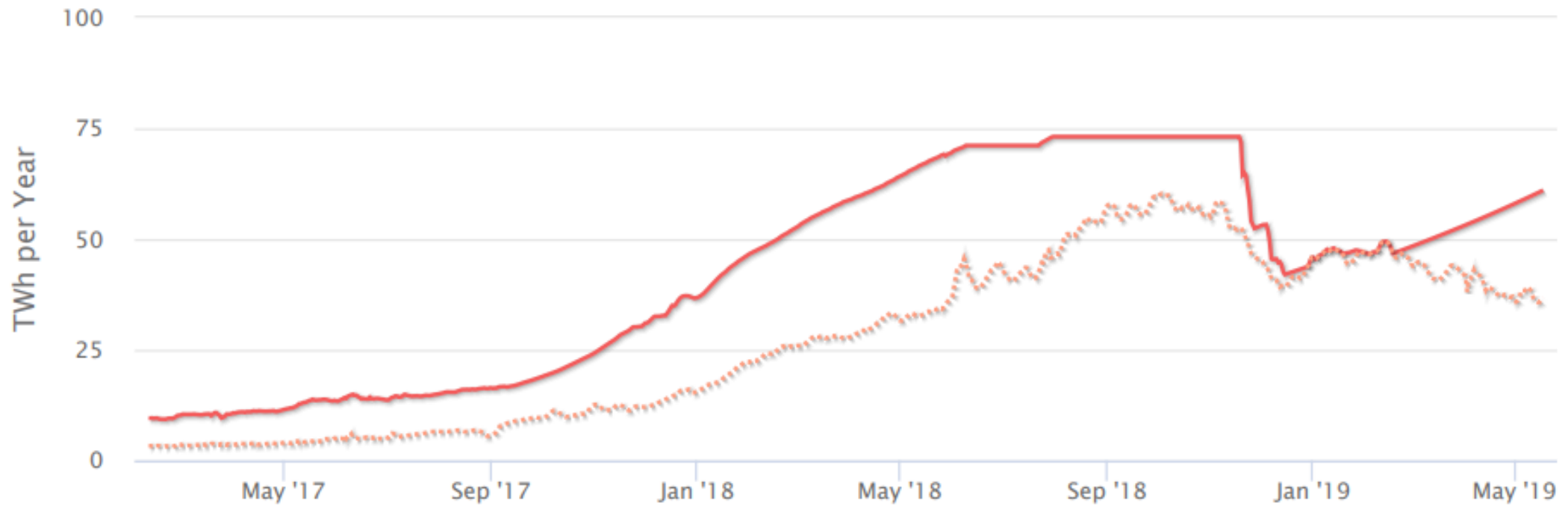
- 블록체인OS의 BosCoin은 presale에서 17시간만에 \$1,200만 모금 (2017.5)
- 더루프의 ICON은 presale에서 6시간만에 4.5만ETH 모금 (2017.9)
- 글로스퍼의 Hycon은 1차 ICO에서 8시간만에 3500BTC 모금 (2017.9)

- 새로운 화폐가 생성되는 과정(조폐)에서, 생성자들(채굴자들)에게 "일을 했다는 것을 증명(proof of work)"하는 것을 강제하여 화폐의 가치와 보안을 보장하는 방식
- 장점: 안정성 - 최초의 P2P방식의 분산원장 방식, Bitcoin Core는 아직 해킹되지 않았음.
- 단점:
 - 거래량/거래속도의 제한
 - Bitcoin은 3~4 tps, Ethereum 20 tps, paypal 200 tps, Visa Card: 2,000 tps
 - 에너지소모 과다 (비트코인 거래 1회당, 미국가정 하루 평균 9.36가구 의 전력량 소비)

Bitcoin Energy Consumption Index Chart



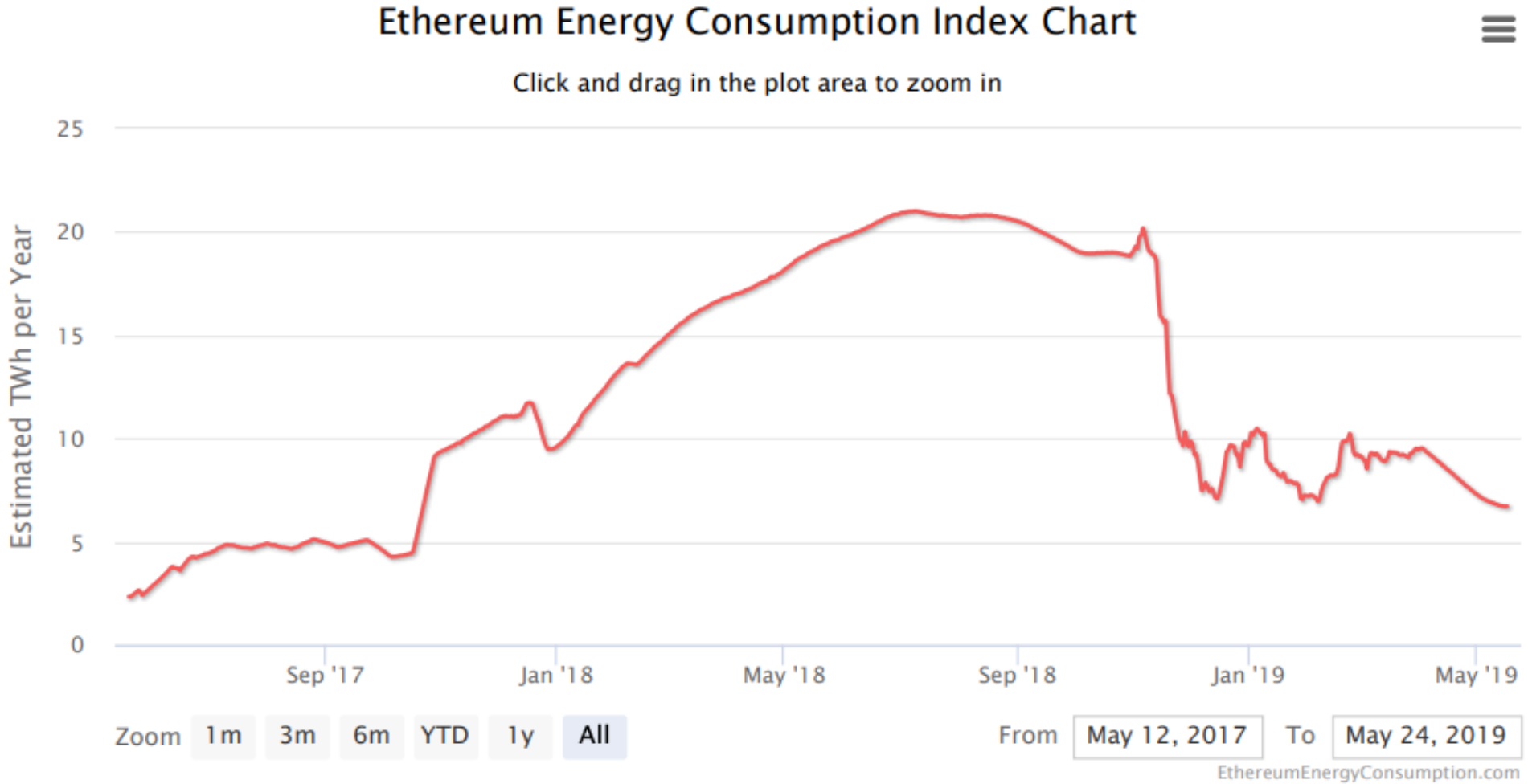
Click and drag in the plot area to zoom in

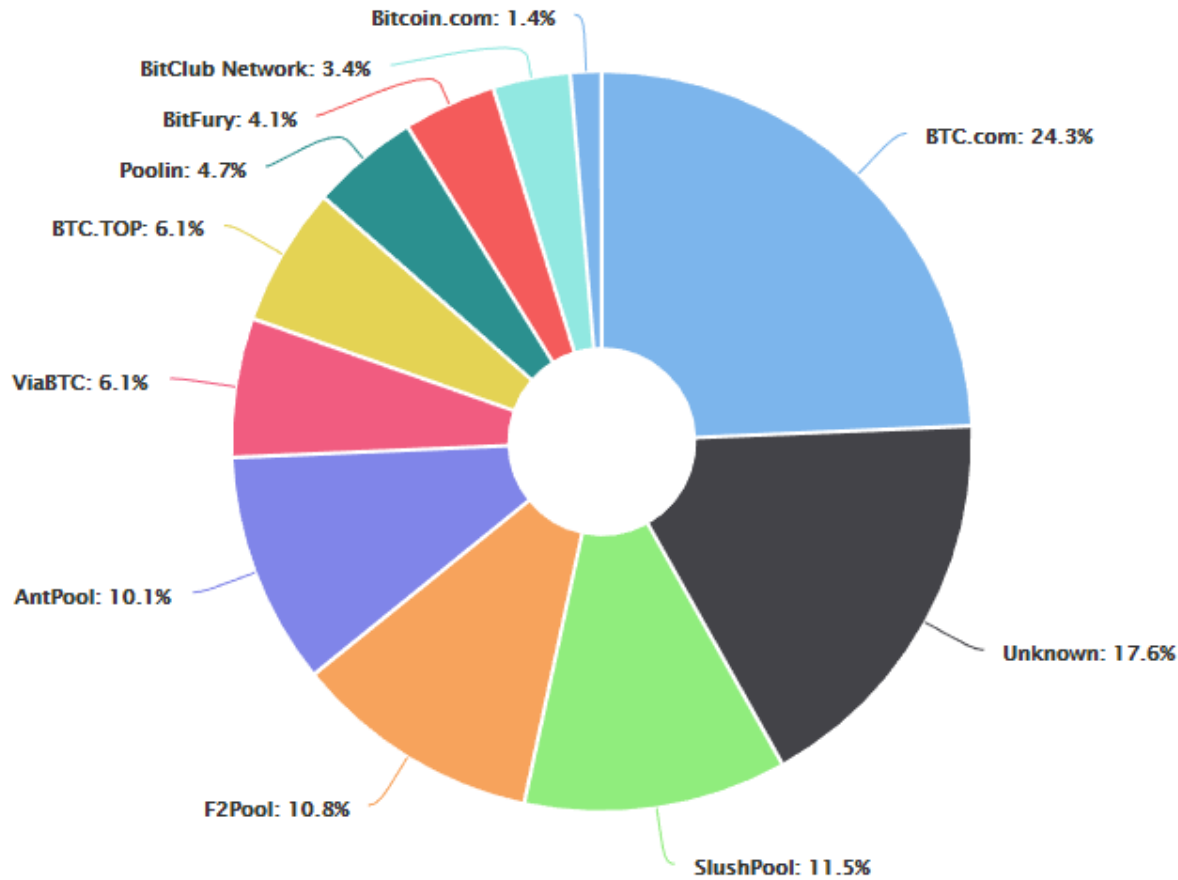


Zoom 1m 3m 6m YTD 1y All

From Feb 1, 2017 To May 25, 2019

Estimated TWh per Year Minimum TWh per Year





Known Blocks.

Relayed By	count
BTC.com	36
Unknown	26
SlushPool	17
F2Pool	16
AntPool	15
ViaBTC	9
BTC.TOP	9
Poolin	7
BitFury	6
BitClub Network	5
Bitcoin.com	2

2. 블록체인 플랫폼 : 50+ 블록체인



- Government
- Waste Management
- Identification
- Healthcare
- Enterprise
- Medical
- Music
- Carbon Offsets
- Supply Chains
- Diamonds
- Real Estate
- Fishing Industry
- Fine Art
- Public Utilities
- Tourism
- National Security
- Taxation
- LGBT Rights

- Mobile Payments
- Land Registry
- Gaming
- Energy Distribution
- Railways
- Oil Industry
- Smart Cities
- Journalism
- Advertising
- Endangered
- Species Protection
- Insurance
- Computation



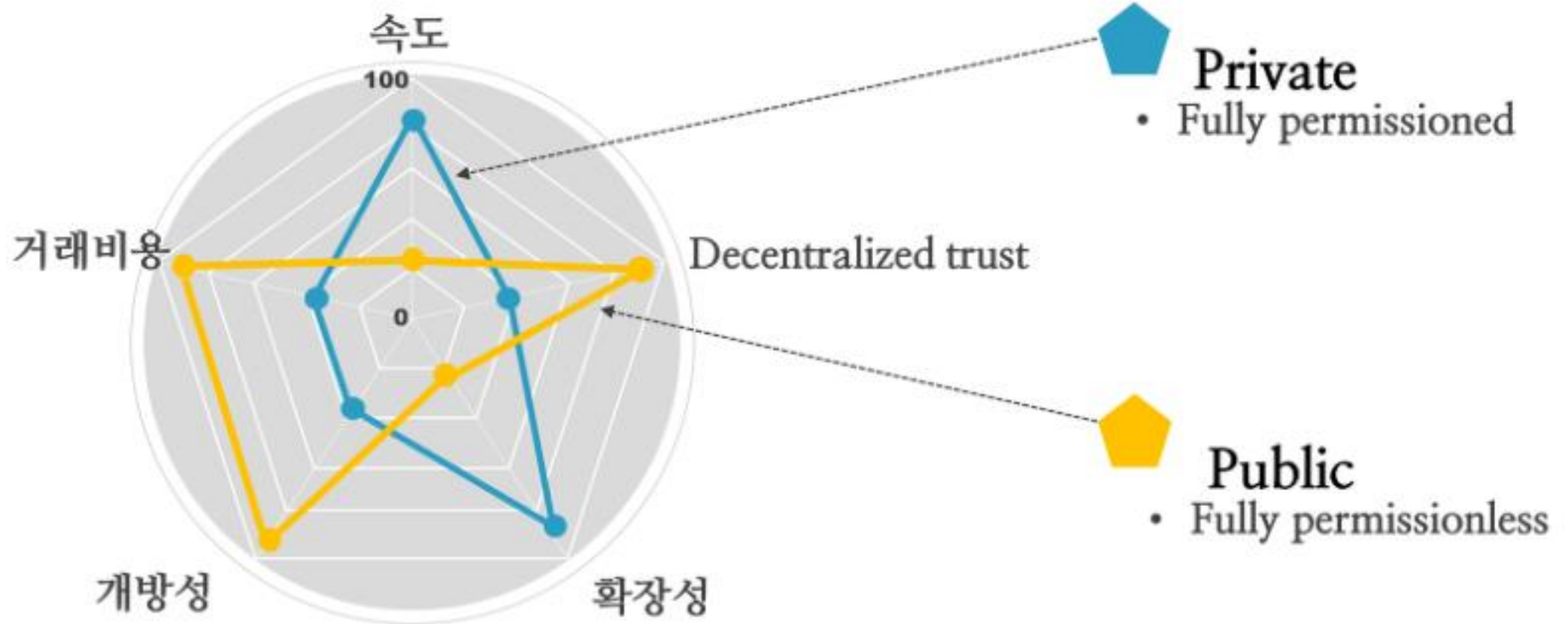
MATTEO GIANPIETRO ZAGO

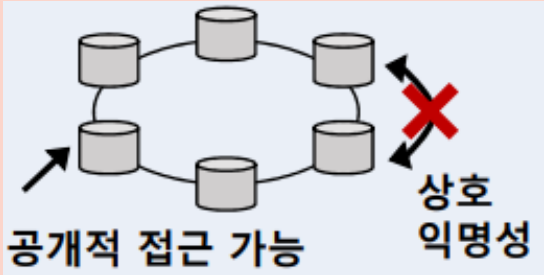
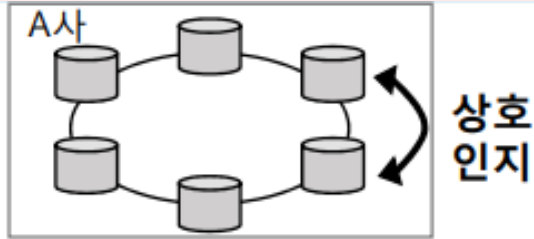
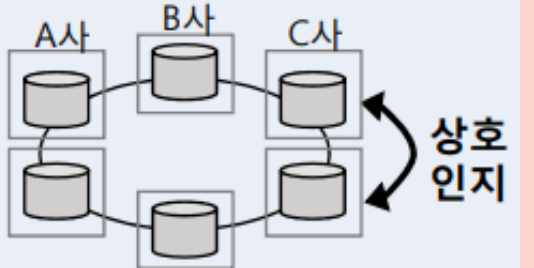
<https://medium.com/@matteozago/50-examples-of-how-blockchains-are-taking-over-the-world-4276bf488a4b>

Public and Private Blockchain

17

	Public blockchain	Private blockchain
접근성	누구나 가능	허가를 받아야 가능
속도	느림(7~20 TPS)	빠름(1000 TPS +)
신원	익명의 노드	확인된 노드
수수료	필수	필요하지 않거나 거의 없음
하드포크	가능	불가능
업그레이드	어려움	쉬움
탈중앙성	높음	낮음
합의알고리즘	PoW, PoS, DPoS 등	BFT 계열
대표 암호화폐	비트코인, 이더리움 등	리플, Fabirc, 아이콘 등



유형 구분	개념 및 특징	구조
<p>퍼블릭블록체인 (Public Blockchain)</p>	<ul style="list-style-type: none"> • 최초의 블록체인 활용사례 • 인터넷을 통해 모두에게 공개 및 운용 • 컴퓨팅 파워를 통해 누구든 공증에 참여 가능 • 네트워크 확장이 어렵고 거래속도 느림 	 <p>공개적 접근 가능 상호 익명성</p>
<p>프라이빗 블록체인 (Private Blockchain)</p>	<ul style="list-style-type: none"> • 개인형 블록체인 • 하나의 주체가 내부자산망을 블록체인으로 관리함 • 해당 체인개발을 위한 플랫폼 서비스 등장 	 <p>상호 인지</p> <p>허가된 사용자만 접근 가능</p>
<p>컨소시엄 블록체인 (Consortium Blockchain)</p>	<ul style="list-style-type: none"> • 반(半)중앙형 블록체인 • 미리 선정된 소수(N개)의 주체들만 참여 가능 • 주체들간 합의된 규칙을 통해 공증 참여 • 네트워크 확장이 용이하고 거래속도 빠름 	 <p>상호 인지</p> <p>허가된 그룹의 사용자만 접근 가능</p>

	비트코인	이더리움	하이퍼레저
분류	퍼블릭 블록체인	퍼블릭 블록체인	프라이빗 블록체인
노드로서 참가자격	누구나 참여가능	누구나 참여가능	멤버십 서비스를 통해 허가된 노드만 참여가능, PKI 기반 증명서 발행
합의 알고리즘	PoW	PoW -> PoS	PBFT/RAFT
결제 완료성	없음	없음	있음
성능	약 10분마다 블록 생성	약 12초마다 블록생성	갱신시 합의를 확정하기 때문에 우수한 성능 보장
트랜잭션 은닉화	트랜잭션 정보는 공개	트랜잭션 정보는 공개	트랜잭션 정보의 공개/암호화를 선택 가능
스마트 컨트랙트	거의 없다시피 함. 제한적인 용도로 사용 가능	이더리움 버추얼 머신(EVM, Ethereum Virtual Machine)에서 동작하는 스마트 컨트랙트 구현 가능. Solidity 언어로 개발	체인 코드(Chaincode)를 통해 스마트 컨트랙트 구현 가능. Go 및 Java로 개발
최소 구성대수	1대부터 가능. 장애 복구를 위해 최소 2대 필요	1대 부터 가능. 장애 복구를 위해 최소 2대 필요	장애 복구를 위해 최소 4대 필요



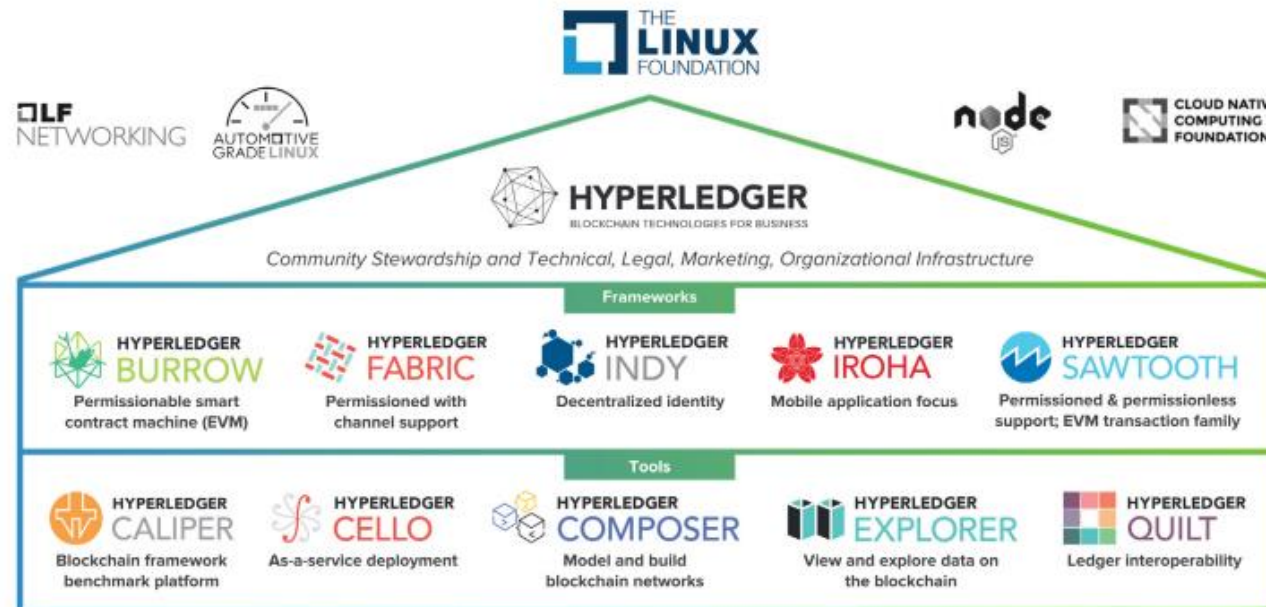
블록체인 플랫폼 : Hyperledger

- 기존 블록체인 시스템 : 낮은 성능, 신원 확인 결여, 무한 경쟁에 따른 과도한 자원 소모
- 기존 블록체인 시스템들에 비해 높은 성능, 신뢰성, 자원 효율성, 그리고 참여자 관리 등 비즈니스 응용의 요구사항을 충족시킬 수 있는 블록체인과 분산 원장(distributed ledger)에 개발에 산업계의 협력 촉진

- 탈 중앙화된 네트워크의 노드들이 검증되고 분산된 장부를 서로 공유함
- 네트워크의 정해진 합의에 따라 데이터들을 보관 및 공유함
- 몇몇 노드들이 잘못되어도 이미 저장된 장부 데이터의 위조 및 변조가 불가능함

- 리눅스 재단(Linux Foundation)
- 프로젝트에는 IBM, 인텔을 포함한 많은 ICT 업체, J.P.Morgan을 포함한 유수의 금융 서비스 관련 업체, SAP을 포함한 많은 비즈니스 소프트웨어 업체 등이 참여

- A project that was initiated by Linux foundation in December 2015 to advance blockchain technology
- A collaborative effort by its members to build an open source distributed ledger framework that can be used to develop and implement cross-industry blockchain applications and systems
- The key focus is to build and run platforms that support global business transactions.
- Projects under the Hyperledger umbrella:





Infrastructure

Technical, Legal, Marketing, Organizational

Ecosystems that accelerate open development and commercial adoption



Frameworks

Meaningfully differentiated approaches to business blockchain frameworks developed by a growing community of communities



Tools

Typically built for one framework, and through common license and community of communities approach, ported to other frameworks



프로젝트	목표
Fabric	모듈 구조를 가지는 분산 응용 플랫폼 개발. 합의 프로토콜, 멤버십 서비스 등의 모듈을 필요에 따라 교체 가능
Sawtooth	경과 시간 증명(Proof of Elapsed Time) 기반의 합의 알고리즘을 적용하여 적은 자원으로 많은 수의 참여자를 지원하는 모듈형 플랫폼 개발
Iroha	패브릭 프로젝트를 모바일 응용 적용에 초점
Burrow	허가형 스마트 계약 해석기를 가지는 모듈 구조의 블록 체인 클라이언트 제공. 허가형 이더리움에 초점
Indy	블록체인 상에서 독립적인 디지털 신원 제공
Explorer	블록체인에 저장된 정보 분석 개발 도구
Composer	블록체인 비즈니스 네트워크와 스마트 계약의 개발과 적용을 돕는 개발 도구
Cello	서비스에 맞는 블록체인을 온-디맨드(on-demand) 방식으로 제공하는 블록체인 생태계 제공
Quilt	서로 다른 블록체인간의 상호동작성(interoperability) 제공

- 목표

- 알려진 참가자를 대상으로 하는 비즈니스 응용 환경에 맞는 블록체인 개발
- 서로 다른 요구사항을 가지는 다양한 분산 응용 개발을 효율적으로 지원할 수 있는 플랫폼 개발
- 모듈 구조를 가지는 분산 응용 플랫폼 개발 -> 합의 프로토콜, 멤버십 서비스 등의 모듈을 필요에 따라 교체 가능 (요구 사항이 다를 수 있기 때문에)

- 현황
 - 하이퍼레저 프로젝트들 중에 가장 먼저 제안
 - 2017년 상반기에 버전 0.6이 발표
 - 2017년 하반기에 버전 1.0이 발표되어 활용
 - 2018년 3월 : 버전 1.1- Node JS chaincode
 - 1.2 : Java Chaincode/1.3 - 1.4 : RAFT Consensus
 - 참여기관
 - IBM이 개발을 주도
 - 엑센추어(Accenture), 인텔, 히다찌, 시스코, 금융 서비스 업체들의 블록체인 컨소시엄인 R3 등
- * RAFT(Replicated and Fault Tolerant) :
- ✓ 기본적으로 복제된 state machine 구조를 가짐
 - ✓ 클라이언트 요청을 하나의 리더 노드가 처리하여 로그를 업데이트하고, 해당 로그가 다른 리플리카에도 반영되도록 하는 형태로 동작
 - ✓ 리더가 문제가 있을 경우, 리더 선출 프로토콜에 따라 리더를 새롭게 선출

- 특징

- 허가형(permissioned) 블록체인
- 일반 프로그래밍 언어(general-purpose programming language) 사용
- 내부 가상통화 부재(no internal cryptocurrency)
- 높은 성능(high performance)
- 교체 가능한 모듈 구조(pluggable modular architecture)
- 멀티 블록체인(multi-blockchain) 지원

- ✓ 누구나 참여할 수 있는 블록체인(이더리움, 비트코인, ...)과 달리 허가된 사용자만 참여할 수 있음
- ✓ 하이퍼레저 패브릭의 Chaincode는 이더리움의 Smart Contract와 유사하지만, 기존의 언어들(Java, Go, Node.js)로 개발할 수 있음
- ✓ 내부적인 메카니즘을 통해 어떤 시스템에서 실행해도 결과가 동일하도록 만듦
- ✓ 초당 10,000 트랜잭션을 처리할 수 있도록 성능을 높이는 것이 목표

• 허가형(permissioned) 블록체인

- 멤버십 관리 서비스를 통해 허가된 참여자만 접근을 허용
- 참여자의 블록체인 접근 권한을 제어 가능
- 참여자 행위에 대한 책임성(accountability) 확인의 요구사항을 반영
- 작업 증명 기반의 합의 알고리즘을 사용하는 대신 보다 효율적인 합의 알고리즘을 사용 가능
- 높은 거래 완료성(transaction finality)

✓ 이 사용자가 등록된 사용자가 맞는지 확인하는 멤버십 관리 서비스

✓ 일반적으로 X.509 Certificate를 발행하는 Infrastructure를 PKI라고 함

✓ X.509 기반의 멤버십 서비스를 제공

✓ 참여자에게 책임을 부여할 수도 있고, 감사를 할 수도 있고, 부인 방지를 할 수 있음

✓ 거래가 승인이 완료되는 즉시, 거래가 완료됨(시간이 지나 블록이 교체가 되는 경우가 발생하지 않도록)

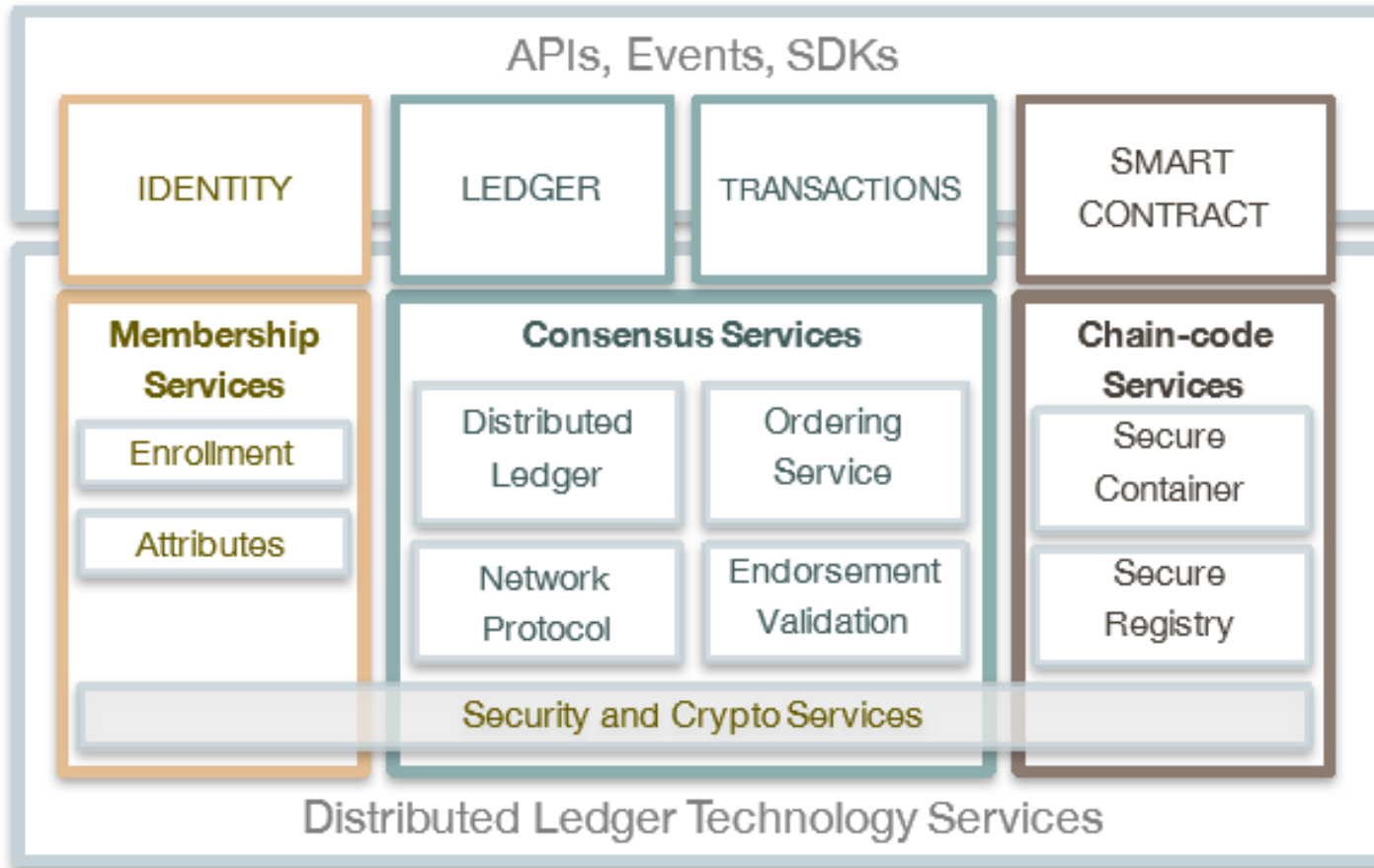
- 비허가형 블록체인과 허가형 블록체인의 비교

구분	비허가형 블록체인	허가형 블록체인
참여자 관리	없음	있음
접근권한 제어	불가능	가능
책임성	없음	있음
합의 알고리즘	작업 증명	비작업 증명 유형
거래 완료성	낮음	높음

- **일반 프로그래밍 언어(general-purpose programming language) 사용**
 - 체인코드(chaincode) : 하이퍼레저 패브릭의 스마트 계약 프로그램
 - 이더리움 : 모든 피어(peer)의 블록체인에서 실행된 스마트 계약의 결과가 항상 동일한 것을 보장하기 위해 결정적(deterministic) 프로그래밍 언어를 특별히 개발하여 사용(예: Solidity)
 - 하이퍼레저 패브릭 : Go, Java 등 일반적인 프로그래밍 언어 사용
- **교체 가능한 모듈 구조(pluggable modular architecture)**
 - 하이퍼레저 패브릭은 전체 시스템을 모듈 구조로 설계하고, 합의 알고리즘 등 응용에 따라 요구사항에 차이가 큰 모듈을 필요에 따라 교체 가능
 - 합의 프로토콜 : SOLO, Kafka, PBFT(Practical Byzantine Fault Tolerant) 등

- **멀티 블록체인(multi-blockchain) 지원**

- 전체 시스템을 다수의 채널(channel)로 구분
- 채널별로 별도의 독립적인 블록체인 유지 가능
- 참여자는 특정 채널에 가입함으로써 공유할 블록체인을 선택할 수 있고, 다수의 채널에 가입 가능



IDENTITY

Pluggable, Membership, Privacy and Auditability of transactions.

LEDGER | TRANSACTIONS

Distributed transactional ledger whose state is updated by consensus of stakeholders

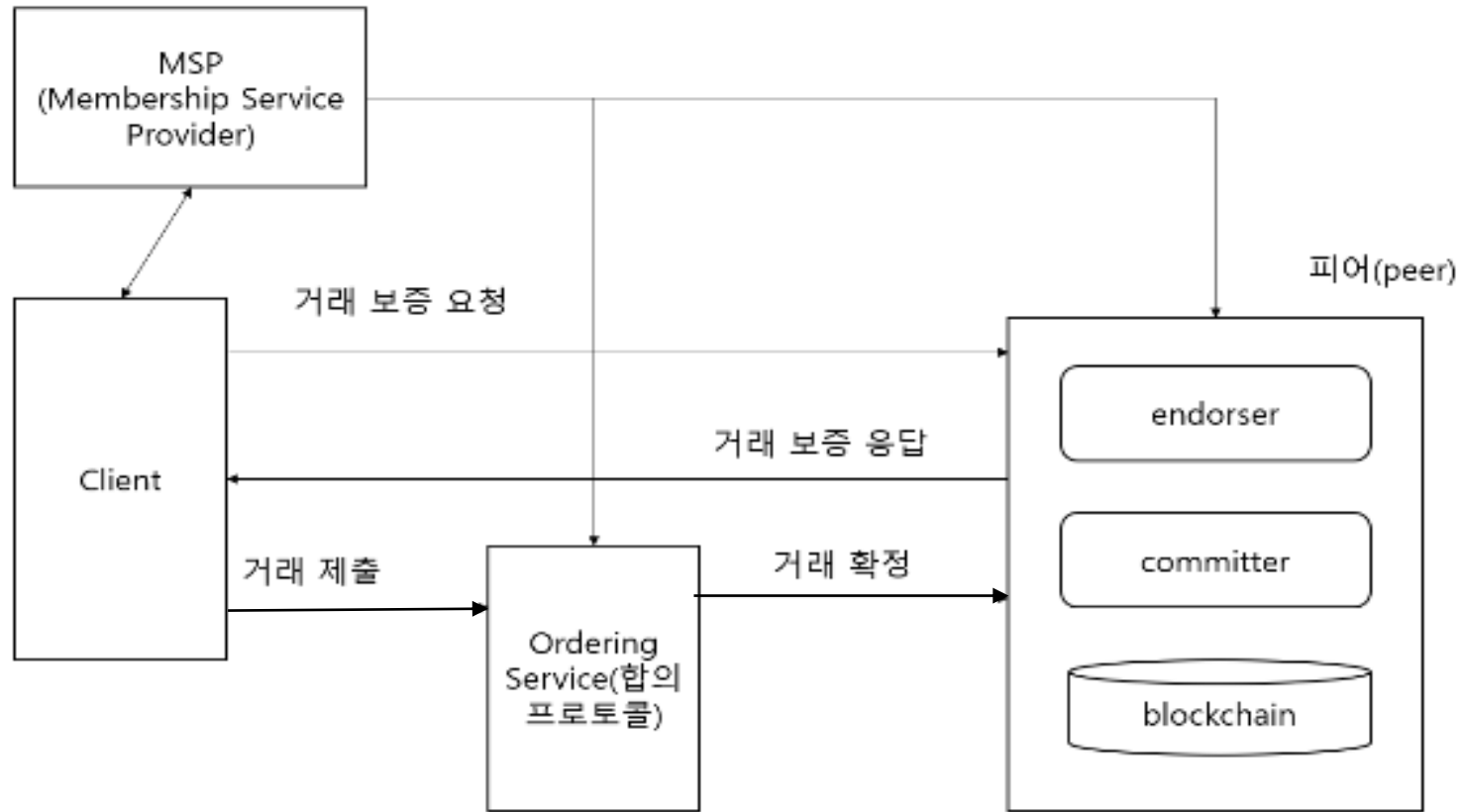
SMART-CONTRACT

“Programmable Ledger”, provide ability to run business logic against the blockchain (aka smart contract)

APIs, Events, SDKs

Multi-language native SDKs allow developers to write DLT apps

- '스마트 계약'(Smart contract)은 프로그래밍된 조건이 모두 충족되면 자동으로 계약을 이행하는 '자동화 계약' 시스템이다.
- A chaincode typically handles business logic agreed to by members of the network, so it may be considered as a “smart contract”. State created by a chaincode is scoped exclusively to that chaincode and can't be accessed directly by another chaincode..



- MSP : 시스템에 참여하는 멤버들의 신원을 확인하고 접근 권한을 관리
- endorser : 거래실행 결과를 블록체인을 유지하는 다른 노드들에게 보내줌
- committer : 거래를 확정시켜서 블록체인을 유지

• 클라이언트 노드(client node)

- 사용자를 대신하여 거래(transaction)를 생성하여 체인코드 실행을 호출하는 노드
- 클라이언트 노드는 거래를 생성하여 보증 피어 노드(endorsing peer node)에게 제출(submit)함으로써 거래 보증을 요청하고 거래 보증 응답을 수집
- 거래 보증 응답을 수집한 클라이언트는 거래 제안(transaction-proposal)을 생성하여 순서화 서비스 노드에게 전달

• 피어 노드(peer node)

- 피어 노드는 거래를 확정(commit)
- 거래 정보를 저장하는 레저(ledger)와 거래 실행 결과에 따른 상태 정보를 저장하는 상태 저장소(state store)로 구성되는 블록체인 유지
- 순서화 서비스 노드(ordering service node)로부터 블록 형태로 거래와 상태 갱신 정보 수신
- 일부 피어 노드는 추가적으로 보증 노드(endorsing peer) 역할을 수행
- 보증 노드는 클라이언트의 보증 요청에 따라 해당 체인코드를 실행하고 결과를 보증하는 역할을 수행
- 보증 노드와 보증 방법은 해당 체인코드와 연계된 보증 정책에 의해 결정
- 보증 정책은 체인코드와 함께 작성되어 체인코드가 블록체인에 배치될 때 함께 배치

- **순서화 서비스 노드(ordering service node)**

- 합의 알고리즘에 따라 클라이언트들로부터 제안되는 거래들을 순서화시켜 피어 노드들에게 안전하게 전달
- 클라이언트는 채널을 통해 거래를 포함하는 메시지를 순서화 서비스 노드들에게 전달하고, 순서화 서비스 노드들은 거래 메시지들을 순서화시켜 채널에 연결된 모든 피어들에게 전달
- 각 피어에게 전달되는 거래 메시지들이 동일한 순서를 가지고 안전하게 전달되는 것을 보장하는, 원자적 브로드캐스트(atomic broadcast) 서비스 제공

- **멤버십 서비스 제공자(MSP-Membership Service Provider)**

- 하이퍼레저 패브릭에 접속하는 노드의 신원 확인 후 네트워크에 접속할 수 있는 권한을 표시하는 자격증명(credentials)을 발급
- PKI(Public Key Infrastructure) 기반의 인증 기관(Certification Authority)을 통해 서비스에 맞는 공개키 인증서(public key certificate)와 대응되는 개인키(private key)를 자격증명으로 발급

- Hyperledger fabric을 구성하는 주요 구성요소
 - Hyperledger Fabric SDK
 - 클라이언트용 Software Development Kit
 - Hyperledger Fabric 기능 사용을 위한 API 탑재
 - ✓ Hyperledger Fabric 네트워크 기동
 - ✓ 트랜잭션 실행
 - Organization
 - Hyperledger Fabric네트워크에 참가하는 조직을 의미하는 논리적 단위
 - 각 Peer와 Orderer는 Organization에 소속

- Hyperledger fabric을 구성하는 주요 구성요소

- Peer

- Organization내 노드를 의미하는 논리적 단위
 - 블록체인, State DB, 체인코드 보유
 - Endorser와 Committer 역할 수행
(성능적 부분을 고려하여 Committer로만 동작하는 경우도 있음)
 - ✓ Endorser : 클라이언트로 부터 요청 받은 트랜잭션 동의(Endorsement)
 - ✓ Committer : 트랜잭션과 실행 결과의 타당성을 확인하여 블록체인과 State DB 갱신

- Orderer

- 동의된 트랜잭션 결과를 블록체인과 state DB에 작성하는 순서 제어

- State DB

- 트랜잭션 실행 결과를 얻어 최신 state를 보존하는 데이터 저장소
 - 체인코드가 State DB를 갱신 중일 때 다른 체인코드의 액세스 불가

- Hyperledger fabric을 구성하는 주요 구성요소

- Channel

- 하나의 Hyperledger 네트워크를 논리적으로 분할할 네트워크
 - 하나의 네트워크에 복수의 독립된 채널 존재 가능
 - 각 채널내에서 동일한 분산원장 유지
 - Consensus takes place within a channel by members of the channel
 - ✓ Other members on the network are not allowed to access the channel and will not see transactions on the channel

Q & A

