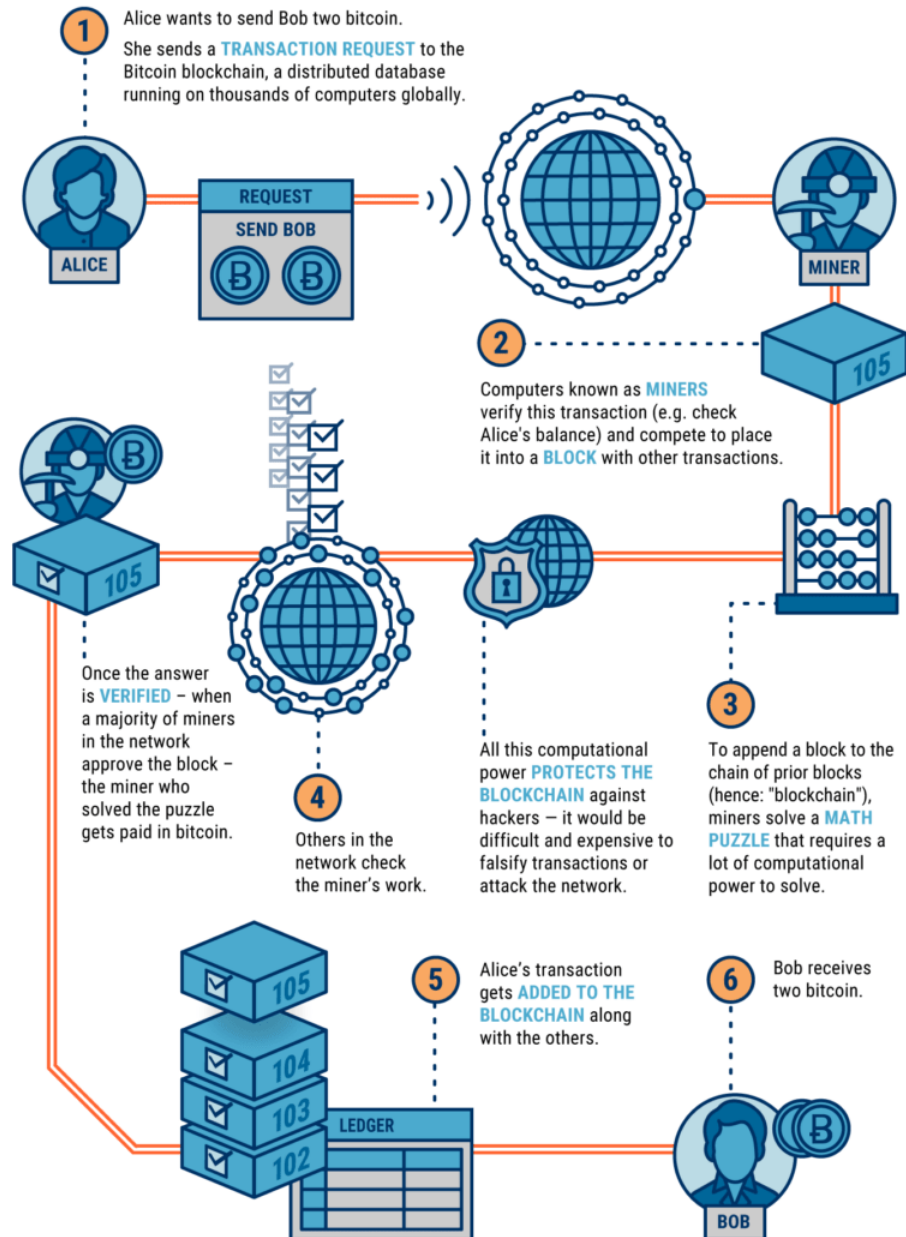


Blockchain



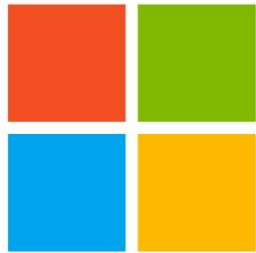
Understanding a bitcoin transaction

HOW BLOCKCHAIN TECHNOLOGY POWERS BITCOIN





IBM LEADS THE WAY WITH 1,500+
EMPLOYEES WORKING ON BLOCKCHAIN



Microsoft

Microsoft captures 19% market share,
second only to IBM



Mark Zuckerberg mentioned
cryptocurrency when he disclosed his
annual project for 2018



AWS' blockchain-as-a-service (BaaS) offering

ORACLE®



Tencent
腾讯

세계 블록체인 시장은 향후 5년간 10배 이상 성장할 것으로 전망

'25년이면 전 세계 총생산의 10%가 블록체인 기술로 저장될 것('16, WEF)

블록체인 유관시장은 '25년 1,760억불, '30년 3조 1,600억불로 성장('17, 가트너)

블록체인 기술은 거래비용 감소와 데이터 위변조 방지가 장점이며,
다양한 산업과 결합하여 효율성을 높이고 새로운 경제적 가치 창출 가능

* 1세대(가상통화/'09~'14) → 2세대(스마트계약 분산앱/'15~현재) → 3세대(확장성 상호운용성/향후)

① 금융 분야

- 비상장 주식 거래
- 실손 보험금 청구

② 의료 분야

- 개인 의료정보 관리
- 유전체 정보 공유

③ 콘텐츠 분야

- 디지털 음원 유통
- 사진 저작권 관리

④ 공공 분야

- 전자증명서 유통
- 온라인 투표

⑤ 물류 · 유통 분야

- 개인 통관
- 다이아몬드 유통

⑥ 에너지 분야

- 이웃 간 전력 거래
- 전기자동차 충전

① 금융 : 대표적인 제3의 신뢰기관인 금융기관의 역할 변화

- 블록체인으로 인해 금융산업의 획기적 변화 예상, “대부분의 은행은 10년 안에 없어질 것이다.” (데이비드 여맥 뉴욕대 교수, '18)

비상장주식을 안전하고 빠르게 거래 (美나스닥, '15)

- △ 비상장주식은 매도자와 매수자 간에 돈과 주식을 교환(직접거래 또는 계좌이체)하거나 중개업체를 거쳐 거래가 이루어지며, 결제 및 장부 반영에 2~3일 시간 소요
- ☞ 장외 주식거래에 블록체인 기술을 적용, 거래소요 시간을 10분 이내로 단축하고, 주식 발행 회사는 주주 현황과 투자자본 흐름을 실시간으로 파악 가능

손쉽게 청구하는 실손보험금 (교보생명, '17)

- △ 진료기록사본 등을 병원에서 발급받아 보험사에 제출하는 절차가 번거로워 청구 금액이 소액인 경우 보험금 청구 포기 사례 다수 발생
- ※ 1만 원 이하 진료비 보험금 미청구 비율 51.4%(15 보험연구원 설문조사)
- ☞ 실손보험금 가입자가 병원에서 진료비를 수납하면 병원과 보험사가 진료기록을 실시간 공유*하여 별도 서류제출 없이 자동으로 보험금 청구가 이루어짐
- * 블록체인 기반 통합인증으로 보험금 청구 및 진료기록 전송이 바로 이루어짐

② **의료** : 개인의 의료주권 확보 및 헬스케어 연관산업 활성화

- 블록체인으로 자신의 의료정보를 보다 안전하고 편리하게 활용하여 의료정보 주체 중심의 신규 헬스케어 비즈니스 창출 유도

내가 직접 관리하는 의료정보 플랫폼 (M社, '18개발중)

“사람들은 하나의 병원만 다니지 않는데, 의료기관끼리 데이터 공유가 힘들다.” - M社 대표

△ 병원마다 **의료정보를 각각 관리**하며, 나에 대한 검사 결과를 DVD(예 : CT·MRI)나 인쇄물(예 : 피검사)로 제공받을 수 있어 **보관·활용이 어려운 현실**

* 의료기관 간 진료정보 교류사업의 경우 환자는 열람할 수 없고 3만여 개 병의원 중 1,322곳 가능(17)

☞ 의료정보를 개인이 스마트폰을 통해 직접 관리할 수 있어 불필요한 **중복검사를 방지**하고, 언제 어떤 검사·진료를 받았는지 등 **의료정보의 체계적 관리** 가능

③ 콘텐츠 : 콘텐츠 유통체계 변화 및 저작권 보호 방안 제시

- 직접적인 콘텐츠 보상체계 마련 및 신뢰성 높은 저작권 보호로 창작자 중심의 콘텐츠 관리, 유통 및 정산의 새로운 변화 주도

수익도 높고 지급도 빠른 투명한 디지털 음원유통 (英Ujo Music, '17)

“음악만으로 돈을 벌 수 없는 가요계 수익구조를 바꿔야 한다.” - 가수 L씨

△ 음원시장 수익 배분은 제작사 및 유통사 중심이며 **저작권자와 실연자**(가수·연주자)의 비중이 낮고 **매 월 단위로 정산**하여 지급하는 형태

☞ 투명한 음원유통 기록 관리로 음원 유통, 저작권자·실연자의 **수익이 두 배 이상 증가**하고 이용자가 음원을 구매하면 **바로 수익 배분** 가능

④ **공공** : 공공서비스의 편의성, 신뢰성 확보 및 국민 참여 확대

- 블록체인으로 공공서비스의 신뢰성 제고, 불필요한 행정 비용 절감, 민간의 직접 참여 확대 등 공공부문 혁신

모바일로 발급받고 제출하는 간편한 전자증명서 (행안부, '18개발중)

△ 주민등록등본 발급은 인터넷으로 편리하게 가능하나, 제출은 **직접 방문, 우편 송부, 팩스 전송** 등이 필요해 서류를 제출하는 **국민이나 접수받는 기업 모두 불편**

* 행정·공공 기관에서 발급하는 증명서는 2,700여종, '15년 기준 3억 7천만 건 종이증명서 발급

☞ 주민등록등본 등 각종 증명서를 전자파일 형태로 발급받은 후 요청기관에 직접 전송(다운로드 받을 수 있는 주소 전달)할 수 있어 **시간 절약과 종이사용 절감** 가능

편리하고 믿을 수 있는 온라인투표 (선관위, '18개발중)

△ 선관위는 학교·아파트 등의 신청을 받아 스마트폰·PC 기반 **온라인투표서비스(K-Voting)**를 제공하고 있으나, **해킹·위변조 우려로 공직선거**에는 도입하지 않고 있음

* 선관위 온라인투표는 총 3,786회 활용('18.4월) / (美) 버지니아 선관위는 해킹을 우려하여 **온라인투표 계획 취소**('15), (佛) 총선에서 해킹 의혹 사전 예방을 위해 **온라인투표를 인정하지 않기로 결정**('17)

☞ 온라인투표 정보를 블록체인에 기록, 선거 후보자·참관인 등 **이해관계자가 직접 투개표 과정·결과를 검증**할 수 있어 신뢰할 수 있는 온라인투표 가능

- 해킹·위변조가 불가능한 블록체인의 특성을 활용, **공직선거** 등에 활용되어 **직접 민주주의 구현**에도 기여

⑤ **물류·유통** : 실시간 물류 추적 및 관리 자동화를 통한 혁신

- 다양한 이해관계들이 함께 참여하는 블록체인을 통해 실시간 추적성 확보, 재고 관리 최적화, 진품 확인 등 유통 선진화

“더 빠른 직구”, 신속하게 처리하고 허위 신고도 예방하는 개인 통관 (관세청, '18개발중)

△ 전자상거래 통관은 쇼핑몰 → 특송업체 → 관세청 순으로 진행되며, **3,300만개**(^{'17})에 이르는 **수입 물품 신고**(특송업체)·**확인**(관세청) 과정에 **건당 12시간** 이상 소요

☞ 통관 관련 정보를 쇼핑몰, 특송업체, 관세청이 공유하기 때문에 **실시간 수입 신고**가 가능하고 **저가 신고도 방지**

⑥ **에너지** : 투명한 에너지 거래, 수요관리 최적화 등 에너지 신산업 창출

- 에너지 블록체인을 통해 에너지 거래시스템 구축, 신재생에너지 거래 확산, 미래 에너지 산업 발굴을 촉진할 것으로 전망

이웃 간 실시간 전력 거래 (네덜란드 꺼블마을, '17)

“블록체인 도입으로 전통 전력산업은 위협을 받을 것” - 블룸버그

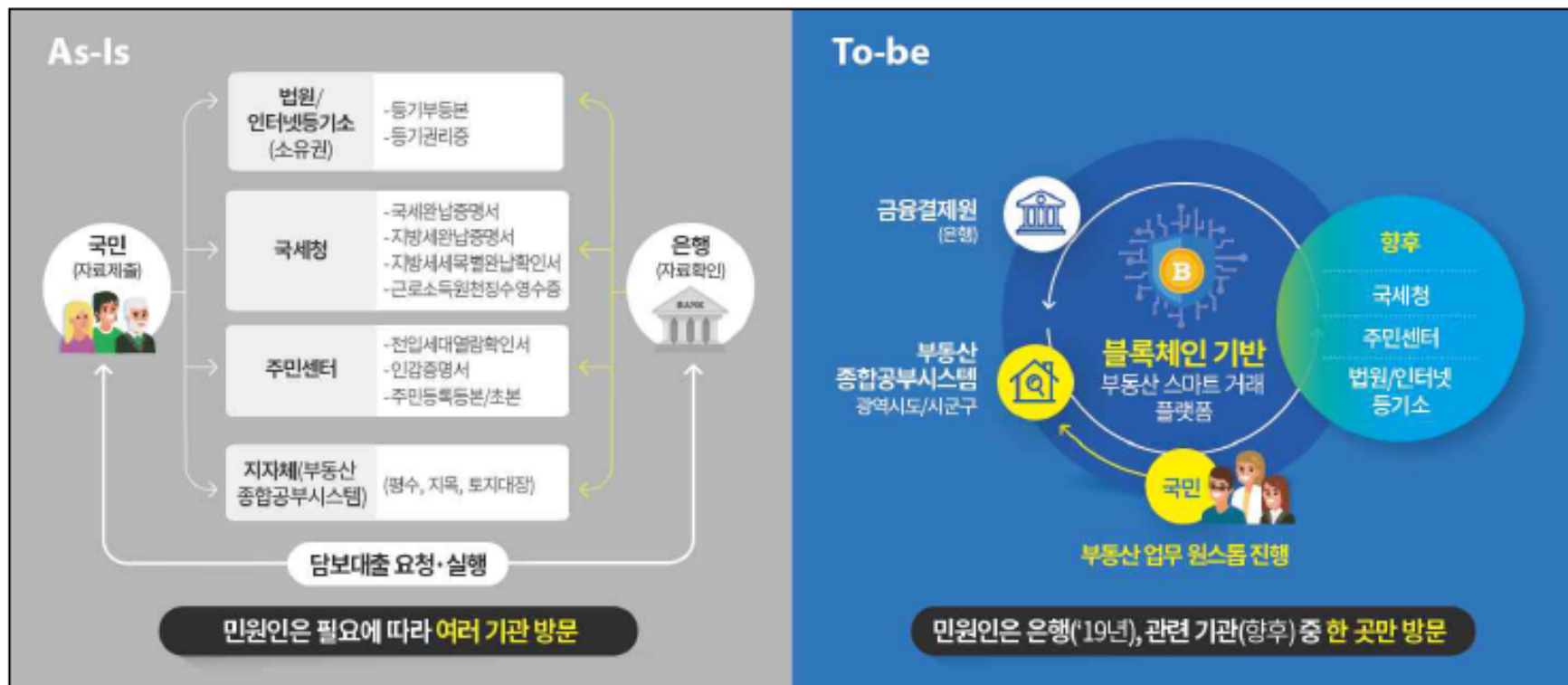
△ 지붕 위에 **150여개의 태양광 패널**을 설치하여 연간 3만6,000kWh의 전력을 생산하고, **여유 전력**을 주고받으며 마을 공동체 내에서 함께 활용

☞ 전력이 남는 집과 부족한 집을 **실시간으로 연결**하고 전력 거래 내역은 블록체인에 기록, 효과적인 전력 배분을 통해 **이상적인 마이크로 그리드 구현** 가능

* 전력 거래에 줄리에뜨(Jouliette)라는 코인이 사용되며, 이 코인은 마을 내 카페에서 음식·음료 구매 가능

□ 간편한 부동산 거래 [국토부]

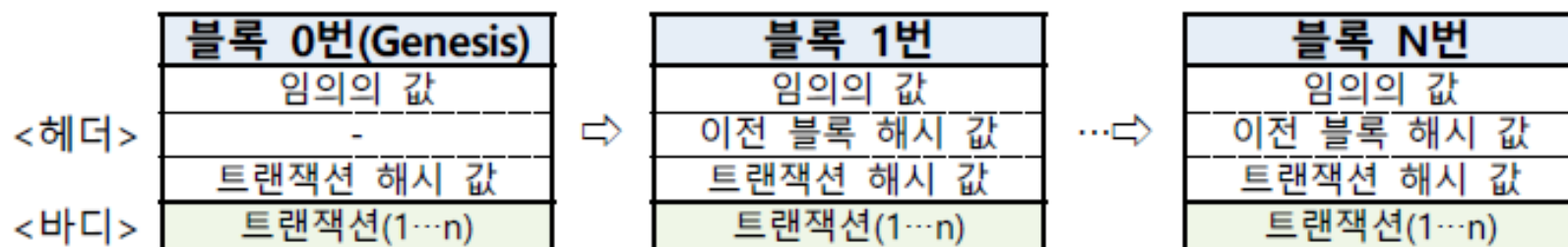
- 부동산 담보대출 요청 시 서류제출을 위해 주민센터, 국세청 등 여러 관계기관을 방문해야하는 번거로움을 관계기관이 함께 참여하는 블록체인 기반 부동산 거래 플랫폼을 통해 해소



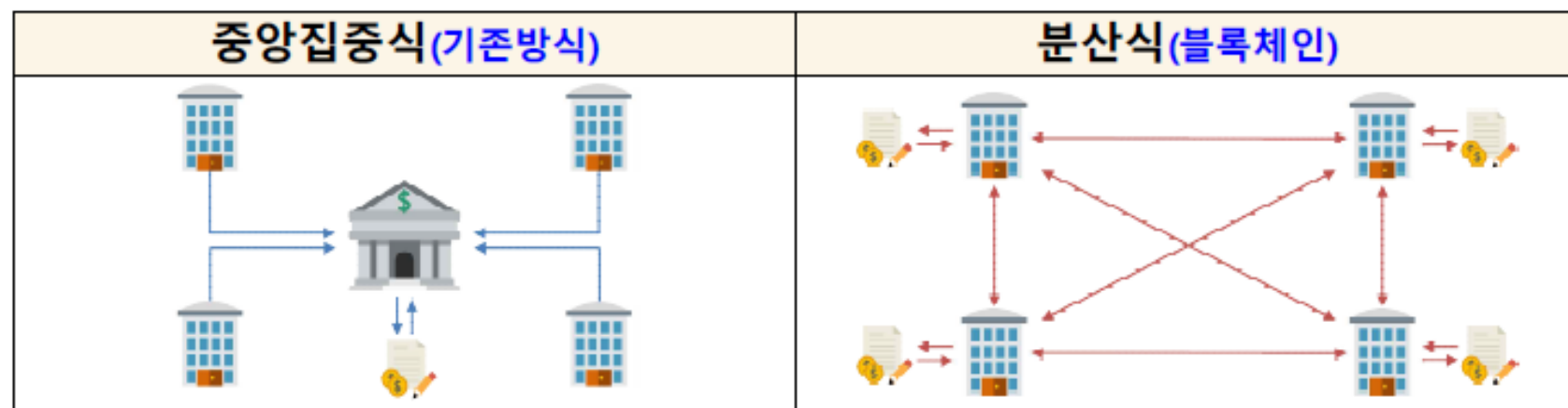
□ 블록체인은 데이터의 신뢰성을 확보하는 기반 기술

- 네트워크 내의 참여자가 공동으로 정보 및 가치의 이동을 기록 · 검증 · 보관 · 실행함으로써 중개자 없이도 신뢰 확보
- 일정 주기*로 데이터가 담긴 블록을 생성한 후 이전 블록들에 체인처럼 연결하는 구조로 이루어져 블록체인이라고 부름
- * 예를 들어 비트코인은 10분마다 합의 과정(작업증명)을 통해 블록을 새롭게 생성

< 블록체인의 구성 형태 >



- 블록체인 기술은 데이터를 중앙집중식으로 관리하던 기존 구조를 탈중앙식·분산식으로 바꾸면서 업무 효율화 및 사회혁신 지향



- 탈중앙식·분산식은 모든 참여자(노드)가 거래내역이 기록된 원장 전체를 각각 보관하고, 새로운 거래를 반영·갱신하는 작업을 공동 수행
 - 데이터 관리기관(은행, 공공기관 등) 운영비용을 절감하고, 해킹에 보다 안전하며, 일부 오류가 발생해도 전체 기능은 동작하는 장애내성이 장점
 - 반면, 참여자들이 함께 합의를 이루고 각자 기록을 관리하는 것이 부담
 - ☞ 빠른 메시지 전파를 위한 P2P 기술 발전, 합의에 필요한 컴퓨팅 성능 향상, 기록 저장을 위한 저장공간 비용 감소로 인해 블록체인 기술의 장점이 부각될 수 있는 여건 조성

Key Characteristics of Blockchain

- *Decentralization*
- *Persistency*
- *Anonymity*
- *Auditability*

CONSENSUS ALGORITHMS

- PoW (Proof of work)
 - hash value of the block header, while varying nonce value
 - When target is achieved, the block is broadcast to all, which validates it and appends to the chain
 - Too much energy is consumed
- PoS (Proof of stake)
 - Miners in PoS have to prove the ownership of the amount of currency
 - Blackcoin, Peercoin, Casper (Ethereum)

- PBFT (Practical byzantine fault tolerance)
- DPOS (Delegated proof of stake)
- Ripple
- Tendermint (byzantine consensus algorithm)
- Many more advanced ones are coming !




- 블록체인은 네트워크 참여에 사전 승인이 필요한지 여부에 따라 퍼블릭 · 프라이빗 블록체인으로 구분 가능

< 블록체인 유형별 주요 특징 >

구분	퍼블릭 블록체인	프라이빗 블록체인
속도	느림	빠름
권한	모든 참여자가 읽기, 쓰기, 합의 등 권한 보유	구성원에 따라 사용 가능한 권한 지정 가능
사례	비트코인(가상통화), 이더리움(가상통화/스마트계약)	코다(금융), 하이퍼레저(범용)

- 블록체인 기술은 단순 지급수단(1세대) 기능에 대한 검증을 거쳐 다양한 거래·계약(2세대)에 적용되며 활용 범위를 넓혀나가는 중
 - (1세대: '09년~'14년) '09년 분산장부 공유 기반 비트코인 등장 이후 블록체인 기술을 활용한 가상통화가 1천 6백여 개 이상 출현('18.6월 기준)
 - (2세대: '15년~현재) 스마트 계약이 추가된 블록체인(이더리움)과 기업의 특정 업무목적에 활용할 수 있는 프라이빗 블록체인 등장
 - 사전에 지정한 조건에 따라 계약이 자동으로 이루어지는 스마트 계약 기능을 통해 상품 주문, 부동산 거래 등 다양한 서비스에 활용 가능
 - 전자문서 공유, 전자거래 등 다양한 산업 분야에서 응용사례 확산
- 앞으로 블록체인 기술은 지금까지의 한계(확장성, 상호운용성 등) 극복을 통해 산업과 사회를 혁신하는 기반기술로 자리 잡을 것으로 전망
 - (3세대: 향후) 기존 중앙집중 방식을 뛰어넘는 성능 개선과 함께 공공 서비스, 계약, 증명 등 신뢰가 필요한 분야에 다양한 혁신사례 창출 기대

< 블록체인 세대별 특징 및 적용사례 >

구분	1세대(2009~2014)	2세대(2015~현재)	3세대(향후)
주요 특징	<ul style="list-style-type: none"> ○ 가상통화 ○ 자산 거래 	<ul style="list-style-type: none"> ○ 스마트계약(비즈니스 자동화) ○ 분산 앱(Decentralized Application) 	<ul style="list-style-type: none"> ○ 확장성(Scalability) ○ 블록체인 간 상호운용성(Interoperability) ○ IoT 지원
대표 사례	○ 비트코인	○ 이더리움 ○ 하이퍼레저	○ 다양한 블록체인 플랫폼 개발 중
개발 현황	<div style="display: flex; align-items: center; justify-content: space-between;"> <div style="width: 30%;">  도입기 </div> <div style="width: 40%;">  확산기  </div> <div style="width: 30%;">성숙기</div> </div>		

< 블록체인 기술개발 로드맵(안) >



구분	과제 명칭	설명
기반 기술	o 고성능 저비용 합의기술	- 트랜잭션 완결성 확보를 통한 고성능과 분산화, 낮은 자원소모를 동시에 만족하는 차세대 합의기술
	o 스마트계약 검증 기술	- 스마트계약의 구현 취약성을 사전에 판단하기 위한 기술로 정형검증 기법* 등을 활용 * 분석대상 시스템의 기능을 논리식과 같은 정형언어로 변환하여 수학적인 증명기법을 적용하는 검증 방식
	o 양자저항성을 가지는 암호기술	- 양자컴퓨팅으로부터 안전한 암호기술을 블록체인에 적용 ※ 양자컴퓨팅은 전통적인 컴퓨터로 풀기 어려워 암호기술에 활용되는 수학적 난제(소인수분해 문제 등)를 보다 빠르게 계산할 수 있는 기술로 블록체인 보안에 위협
확장 기술	o 대용량 데이터 처리 기술, 외부 데이터 연동 기술	- 블록 용량 한계 해결을 위한 기술 및 블록체인 밖의 저장소와 블록체인을 연동하기 위한 인터페이스 기술
	o 대규모 서비스 제공을 위한 확장성 확보 기술	- 다수의 노드 참여 시 분산화와 보안성을 유지하면서 블록체인 네트워크의 성능을 유지시켜주는 기술* * 네트워크 및 트랜잭션 샤딩 기법 통신 오버헤드 최소화 기법 등
	o 상호 운용성 확보 기술	- 서로 다른 이기종 블록체인 간 데이터 거래 호환을 위한 기술, 응용프로그램과 블록체인 호환을 위한 기술
서비스 기술	o 거래 추적 및 분석 기술	- 거래내역 배포 상황 및 블록에 저장된 거래내역의 완결 여부, 이상거래 발생 상황 등을 준 실시간으로 확인 가능한 모니터링 기술
	o 산업 분야별 기존 시스템 연동 기술	- 블록체인과 연동이 요구되는 산업분야별 기존 시스템의 데이터를 블록체인 상에 안전하게 전달하는 위한 기술
	o 전략 서비스 분야별 특화 블록체인	- 전략 서비스 분야에서 상이하게 요구되는 성능, 보안 기능, 외부 호환성을 고려한 맞춤형 블록체인 플랫폼 기술

TRUST

Blockchains have several major technical barriers that make them impractical for mainstream use today

- Limited scalability
- Limited privacy
- Lack of formal contract verification
- Storage constraints
- Unsustainable consensus mechanisms
- Lack of governance and standards
- Inadequate tooling
- Quantum computing threat
- ... and more.

Limited scalability

- **Low throughput:** Blockchains can only process a limited number of transactions
- **Slow transaction times:** The time required to process a block of transactions is slow. For example, Bitcoin block times are 10 minutes, while Ethereum block times are around 14 seconds. These times are even longer during peak moments. Compare that to the nearly instantaneous confirmations you get when using services like Square or Visa.

국가	정책 동향
 미국	<ul style="list-style-type: none"> ○ 블록체인 서비스 활용을 위한 제도 개선, 공공서비스에 블록체인 기술 접목 등 블록체인에 대한 정책적 관심이 증가하는 추세 ※ 버몬트, 애리조나, 네바다 주는 블록체인 기반 전자문서의 법적 효력을 인정, 재무부 등에서 기술 도입을 위한 개념검증 실시
 캐나다	<ul style="list-style-type: none"> ○ 국립과학연구소(NRC)는 정부 보조금 지원 정보를 블록체인을 통해 공개하고 있으며, 추가 시범적용분야 지속 발굴 예정 ※ 캐나다 중앙은행 등은 블록체인 기반의 금융기관 간 결제시스템을 연구('16)
 영국	<ul style="list-style-type: none"> ○ 과학부에서 “분산원장 기술: 블록체인을 넘어(Distributed Ledger Technology: beyond blockchain)” 보고서* 발간('16.1) * 블록체인 기술의 효용성 평가 및 실증사업 추진, 규제 개선, 실제 적용 가능 수준으로 기술력 확보 등을 추진할 것을 권고 ※ 복지예산 관리에 블록체인 기술 적용으로 불필요한 행정절차 및 서류 위변조로 누수되는 복지 예산 2.5~5.4% 절감 기대
 중국	<ul style="list-style-type: none"> ○ 13차 5개년 국가정보화규획에서 블록체인을 중점 육성 기술로 선정('16.12) 하였으며, 지방정부 차원의 산업육성 장려 ※ 항저우시는 블록체인 산업파크(Blockchain Industrial Park)를 조성('17.5) ※ 중국 중앙은행은 블록체인 기반 어음 거래 플랫폼 시범운영
 일본	<ul style="list-style-type: none"> ○ “블록체인 기술을 이용한 서비스 국내외 동향조사(‘16.4)” 보고서를 통해 블록체인 기술의 도입 효과를 분석 ※ 도시·농촌 및 산림지역 토지 등록부, 정부 계약시스템, 식품 안전, 중앙정부와 지방정부 조달을 위한 전자시스템 분야에 블록체인 시범사업 진행('17~)
 UAE(두바이)	<ul style="list-style-type: none"> ○ 블록체인 기반 정부시스템 구축을 위한 전략(Dubai Blockchain 2020 Strategy)을 바탕으로 공공영역 적용* 본격화(‘17~) * 필수 문서의 디지털화로 114백만 톤의 CO2배출량 절감 기대 ※ 두바이 글로벌 블록체인 챌린지 개최(15개국 21개 스타트업 참여, '17)

BITCOIN & BLOCKCHAIN STARTUPS MARKET MAP

WALLETS & MONEY SERVICES



EXCHANGES & CRYPTOCURRENCY TRADING



P2P MARKETPLACES & P2P LENDING



MERCHANT SERVICES



ENTERPRISE SERVICES & CURRENCIES



SOCIAL & BROWSERS



CRYPTOCURRENCY MINING



IoT, IDENTITY & CONTENT MANAGEMENT



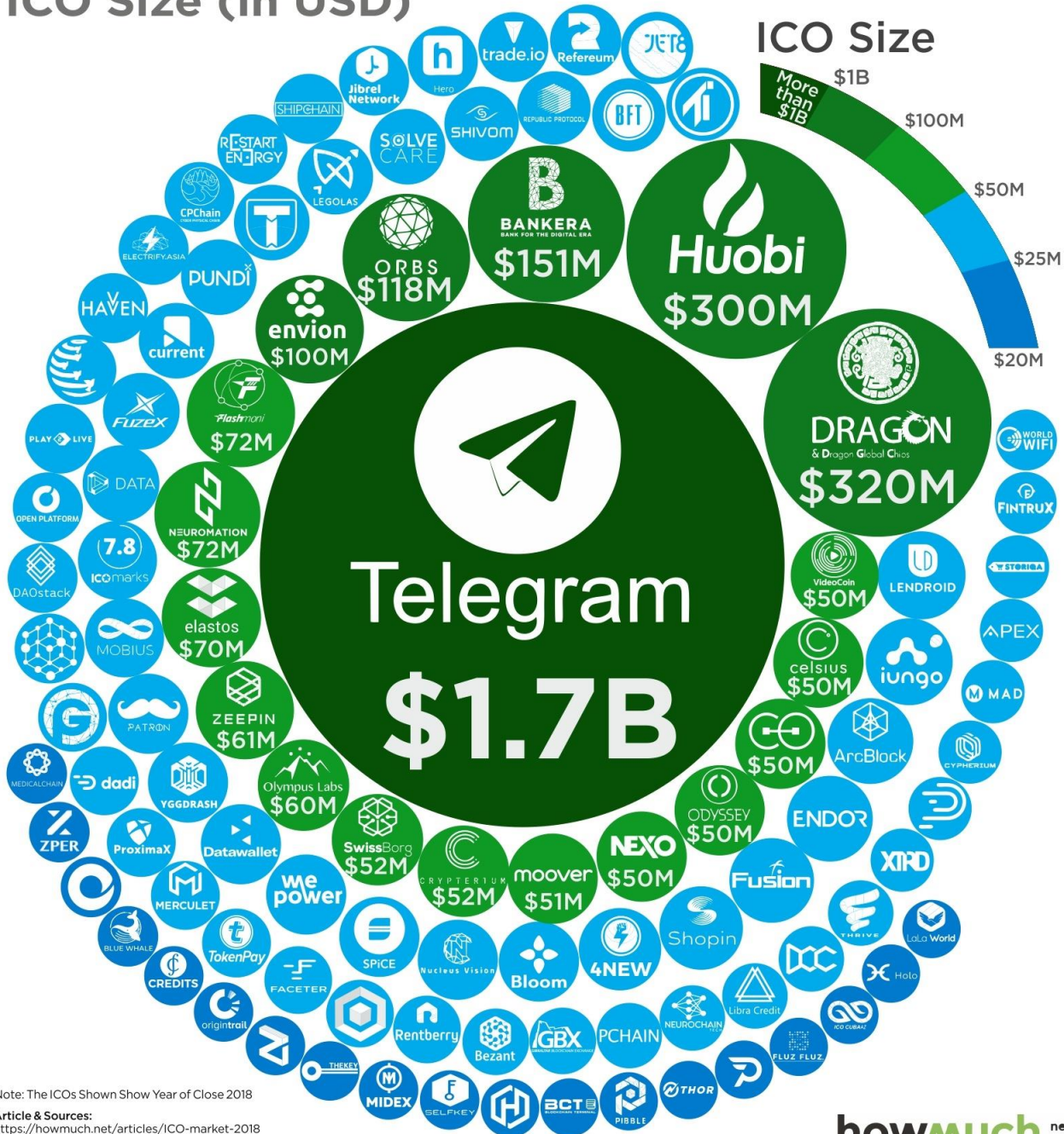
STORAGE, SECURITY & REGULATORY



CAPITAL MARKETS & FINANCIAL SERVICES



The ICO Market in 2018



Note: The ICOs Shown Show Year of Close 2018

Article & Sources:
<https://howmuch.net/articles/ICO-market-2018>
<https://www.coindesk.com/ico-tracker/>