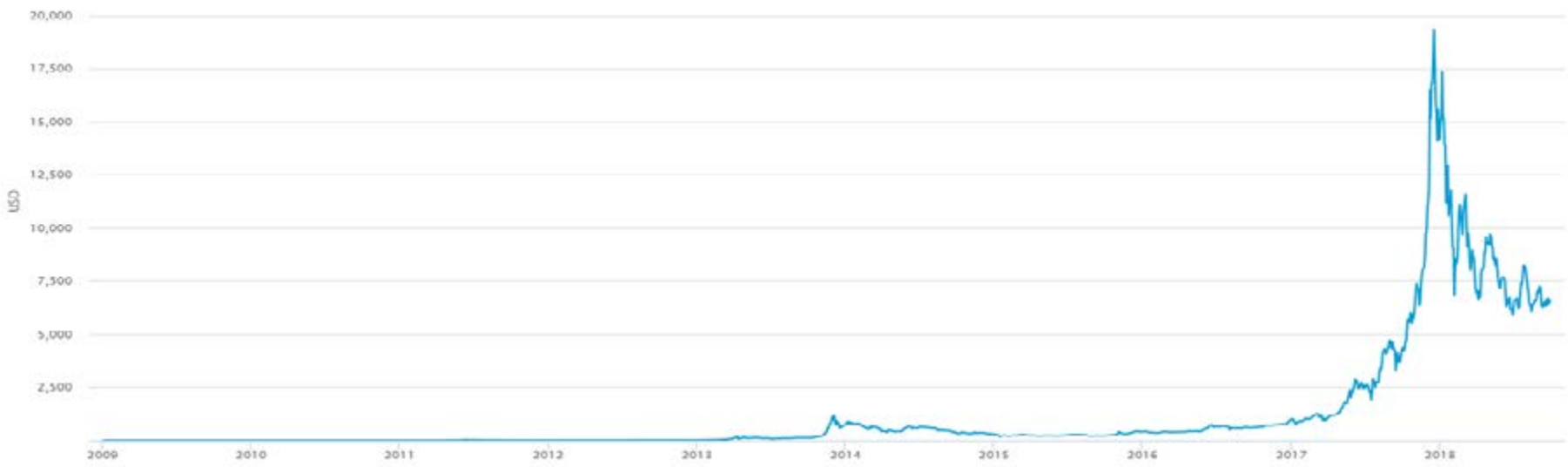
Block-chain Finance

2018. 10. 05 | 최준용 박사

목차

비트코인 가격변동 차트(https://www.blockchain.com 2018-10-02 기준)와 역사



- 2010년 비트코인의 가격은? 5월 22일(피자데이) 피자두판(30달러)/1만 BTC = 현재 740억원
- 2013년 3월 키프로스 사태: 이틀만에 15% 상승(100달러/BTC) 위기 시 안전자산?
- **2014년 2월 26일 일본소재 달러기반 세계 2위 Mt.Gox 거래소 해킹 파산. BTC 70% 폭락**
- **2016년 4월 일본의회 결제수단으로 인정/17년 4월부터 발효(Y화 유입)/9월 과세지침 발표**
- 2017년 9월 중국 ICO 금지 / 한국 ICO 금지 (이미 8월 빗썸 하루 거래량 2조6천억 > 코스닥)
- **2017년 12월 시카고상품거래소(CME)와 시카고옵션거래소(CBOE)에서 선물거래**
- 2017년 12월 비트코인 가격 연초대비 20배(2만$), 한국 전세계 거래 21%차지/김프 40%육박
- **2018년 1월 11일 박상기 법무부 장관 '가상증표' 거래소 폐쇄 언급 → 번복 (현재 신규규제)**
- 2018년 1월 26일 일본 2위의 코인체크 거래소 해킹. (XEM 5.4억 개, 6200억원, 26만명 피해)

Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
October 31, 2008
www.cryptovest.co.uk

Abstract

A purely **peer-to-peer version of electronic cash** would allow online payments to be sent directly from one party to another **without going through a financial institution**. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required to prevent double-spending. We propose a solution to the **double-spending problem** using a peer-to-peer network. The network timestamps transactions by hashing them into an ongoing chain of **hash-based proof-of-work**, forming a record that cannot be changed without redoing the proof-of-work. The longest chain not only serves as proof of the sequence of events witnessed, but proof that it came from the largest pool of CPU power. As long as a majority of CPU power is controlled by nodes that are not cooperating to attack the network, they'll generate the longest chain and outpace attackers. The network itself requires minimal structure. Messages are broadcast on a best effort basis, and nodes can leave and rejoin the network at will, accepting the longest proof-of-work chain as proof of what happened while they were gone.

해시함수(Hash Function)

Deep learning & BitCoin Mining 계산

1 Bit

1bit라도 바뀌면
완전히 바뀜

0123456789abcdef0123456789abcdef0123456789abcdef0123456789abcdef123456789abcdef0123456789abcdef

Md5 ▶ cb3857be6e8fdf053160acc2d247e464

Sha1 ▶ d6e211c1fb03c5a3df37067889ee72becd12ea25

0123456789abcdef0123456789abcdef0123456789abcdef1123456789abcdef123456789abcdef0123456789abcdef

Md5 ▶ 95cf8925ca5f0849f07bde9387390eb0

Sha1 ▶ c049170fd8e39e8b2ddf6352320fb609444cf229

Hash 함수 특징

사이즈가 다른 데이터를 같은 크기의 데이터로 digest함. 따라서 정보가 열화됨

8 Byte	512 KB	1.4 MB	80 GB
사용자 패스워드	스캐너로부터의 영상 데이터	플로피 디스크의 모든 파일	하드 디스크의 모든 파일
			
일방향 해시함수 (SHA-1)	일방향 해시함수 (SHA-1)	일방향 해시함수 (SHA-1)	일방향 해시함수 (SHA-1)
43 B0 4C 54 3B 67 A2 23 3F 7D 36 2B 7A 2B 49 3C D3 AF 27 4A	73 BF 4C 34 3B 67 A2 45 23 76 3F 76 D2 37 F6 44 47 8F 93 D2	43 B0 4C 54 3B 67 A2 23 3F 7D 36 2B 7A 2B 49 3C D3 AF 27 4A	73 BF 4C 34 3B 67 A2 45 23 76 3F 76 D2 37 F6 44 47 8F 93 D2
해시값 **20 Byte**	해시값 **20 Byte**	해시값 **20 Byte**	해시값 **20 Byte**

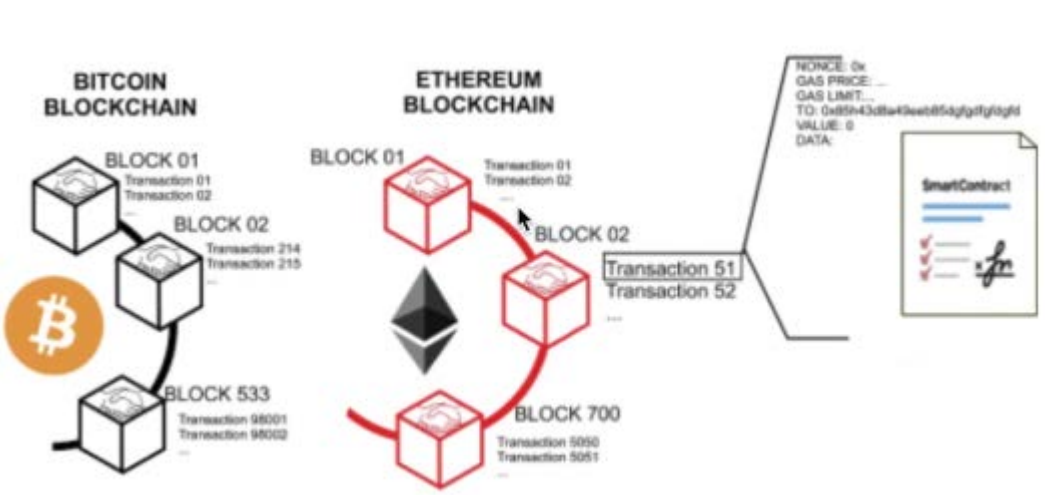
PoW (Proof of Work)

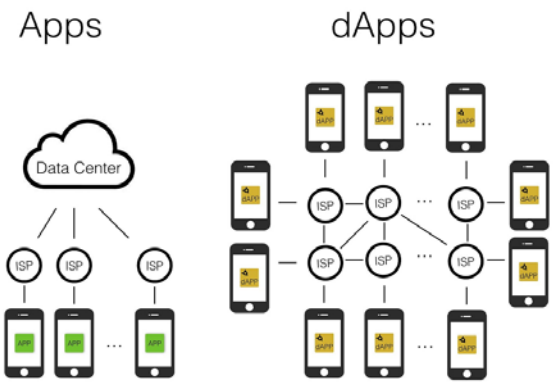
1M byte의 한 블록 당 약 1800개의 거래정보 저장
블록은 10분에 하나씩 생성

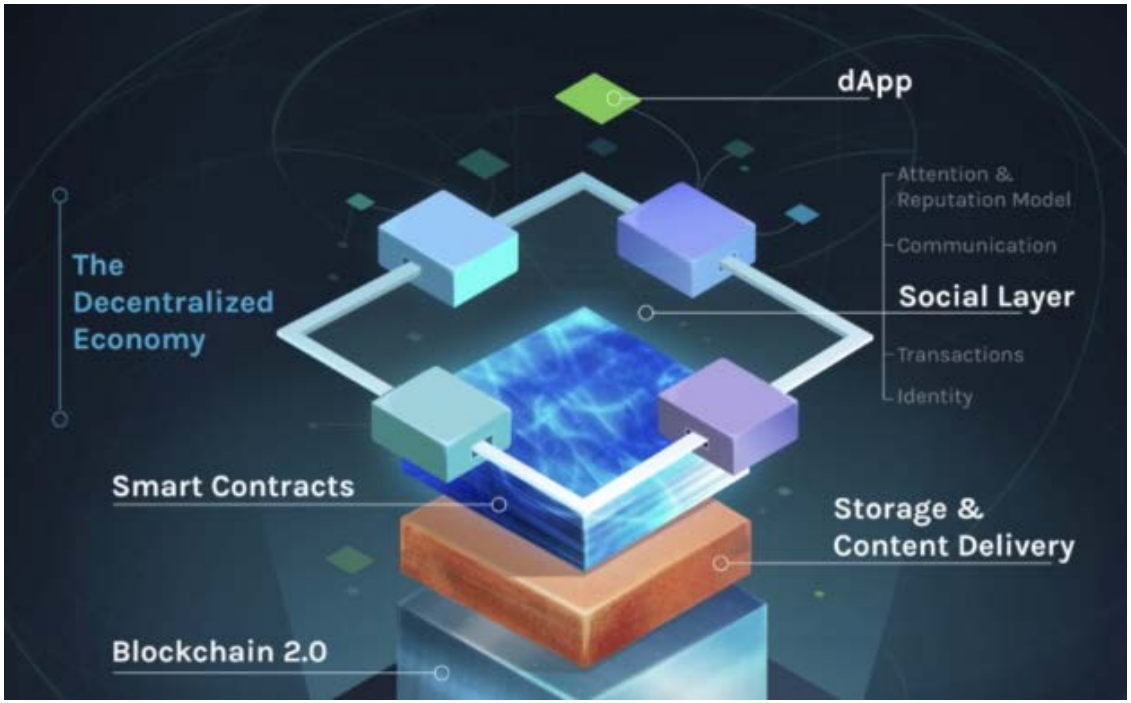
채굴(거래의 기록)의 예

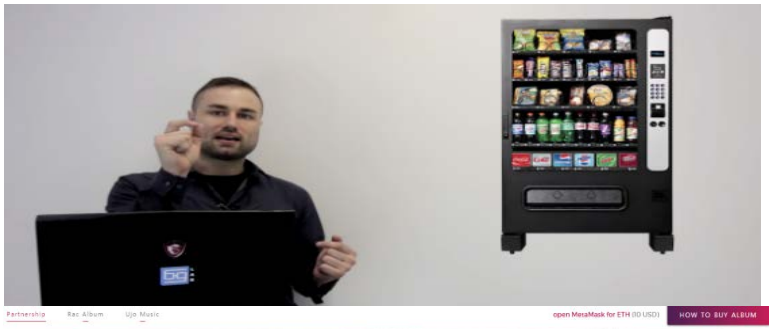
블록해쉬가 000000a84...라는 특정 값보다 작게 나오는 Nonce(Number used once) 값을 찾아라!

이더리움 개발환경과 Token Economy의 시작

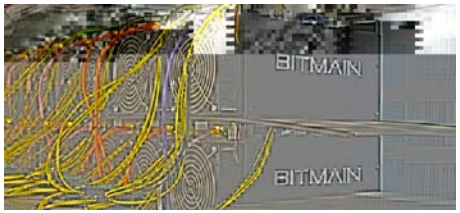


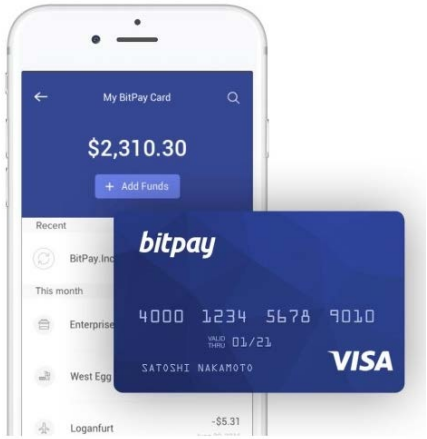






암호화폐 시장의 에코시스템



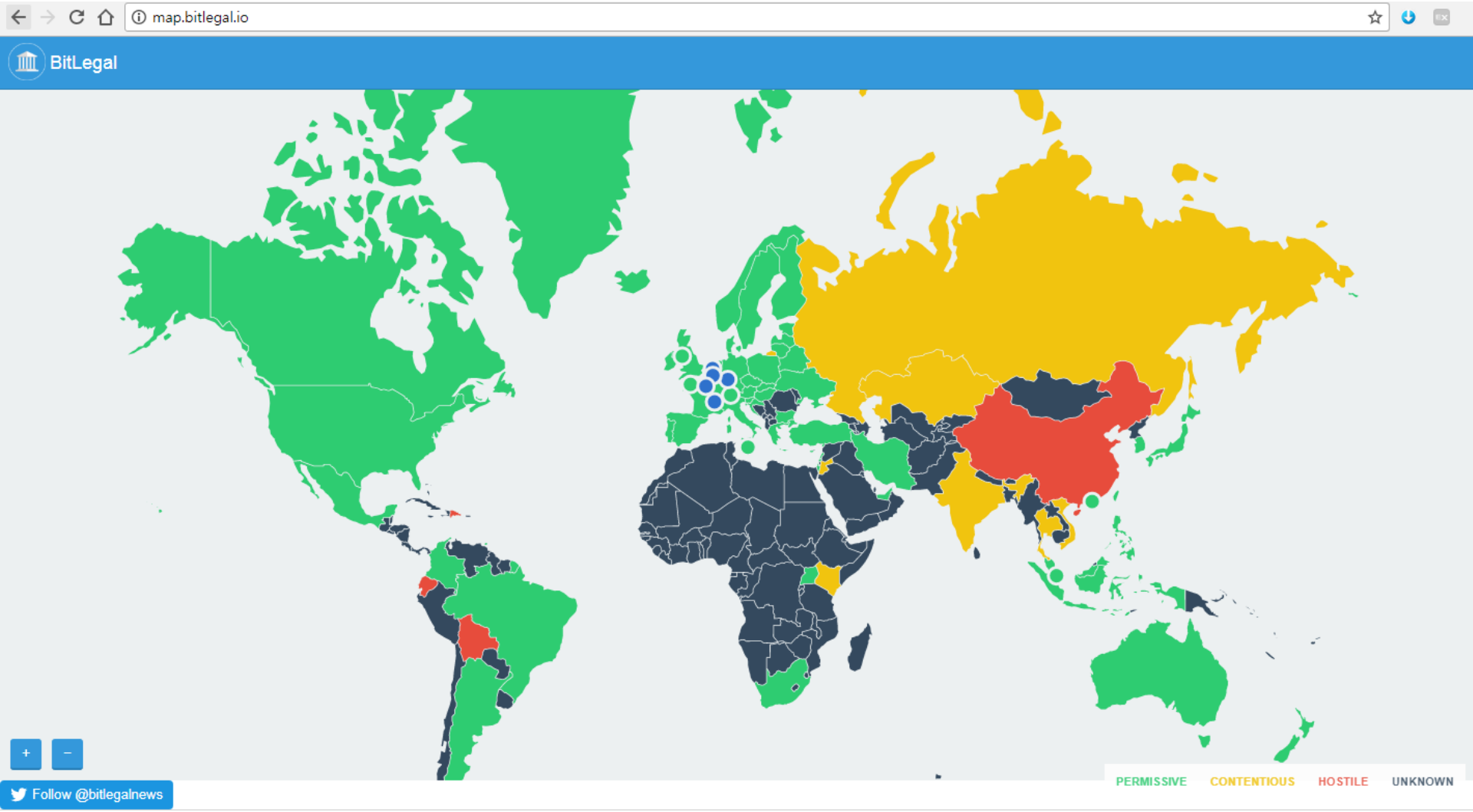


암호화폐의 종류 (https://coinmarketcap.com 2018-10-02 기준)

Total Market Cap: $222,291,628,710

#	Name	Market Cap	Price	Volume (24h)	Circulating Supply
1	Bitcoin	$114,016,912,312	$6,590.61	$3,997,225,995	17,299,912 BTC
2	Ethereum	$23,609,705,371	$230.77	$1,597,501,583	102,309,367 ETH
3	XRP	$22,986,128,946	$0.575583	$1,410,852,653	39,935,410,492 XRP *
4	Bitcoin Cash	$9,226,901,894	$530.91	$450,906,373	17,379,288 BCH
5	EOS	$5,198,761,585	$5.74	$695,607,944	906,245,118 EOS *
6	Stellar	$4,850,431,194	$0.258140	$67,713,139	18,789,958,255 XLM *
7	Litecoin	$3,527,323,312	$60.25	$457,106,909	58,540,377 LTC
8	Tether	$2,797,019,022	$0.996650	$3,070,798,425	2,806,421,736 USDT *
9	Cardano	$2,190,041,127	$0.084469	$42,076,409	25,927,070,538 ADA *
10	Monero	$1,882,501,158	$114.41	$20,642,389	16,453,750 XMR

암호화폐 법적지위의 혼선 (http://bitlegal.io/ 2018-10-02 기준)



화폐? 통화? 자산? 증표? / 암호? 전자? 디지털? 가상? / 양도소득세? 법인세? 거래세?
미국: 암호화된 디지털 자산(asset) / 한국: 가상통화(청)/가상증표(법)
➔ ICO White Paper의 **가장 중요한 부분**으로 암호화폐 설계의 '**Legal Risk Hedging**'이 대두

암호화폐 규제 Vs. 블록체인에 대한 장밋빛 전망

가상화폐 규제

2017년 12월 13일, 대한민국 정부

가상통화 관련 긴급대책(2017.12.13)

가상통화 투기근절을 위한 특별대책 (2017.12.28)

가상 화폐 거래 실명제(2018.1.23)

세계경제포럼(2016)

다보스포럼(2018)

Blockchain technology value to exceed $3.1 trillion by 2030

Mar 3, 2017

Gartner®

Gartner Forecast: Blockchain Business Value, Worldwide, 2017-2030

가트너 (2017)

- (국내) 암호화폐 규제 → 암호화폐 투기 근절을 위한 각종 규제안 마련 및 발표
- (해외)블록체인 기반 플랫폼이 2027년 전 세계 GDP의 약 10%를 차지할 것으로 전망(WEF)
- (해외)블록체인 부가가치는 2017년 40억달러에서 2030년 3.1조달러 이상 급증 전망(가트너)

블록체인 패러다임 전환

정의

블록체인은 기술적으로 거래, 계약 등의 정보가 분산원장 상에 암호화 및 연결되어 저장된 데이터 체인을 뜻하나, 보다 폭넓게는 중앙서버 없이 프로그램의 자기실행(self-execution)이 가능한 분산원장네트워크 및 그에 수반되는 기술 (Buterlin, V.)

패러다임 전환

중앙집중 서비스는 중앙기관(서버 등)의 장애 발생 시 전체 시스템이 정지해야만 하지만, 블록체인은 모든 네트워크 참여자가 정지하지 않는 이상 **영구적으로 지속 가능**함

과거 기록의 위변조를 위해서는 과거 시점 이후의 모든 블록을 다시 생성하고 네트워크의 모든 원장 사본을 교체해야 하므로 **사실상 위변조가 불가**능한 구조

기존 인터넷 상의 거래에서는 중앙관리 시스템이 필요하지만, 블록체인 네트워크 상에서는 **당사자 간(P2P)의 직접적 거래**가 가능해져 산업분야 활용 가능성이 매우 높음 (높은 확장성)

과거 **사이버 패러다임**은 1980~90년대 종이문서와 수작업 중심의 비즈니스 프로세스를 컴퓨터 (전자문서)와 인터넷 중심의 비즈니스 프로세스로 혁신하는 움직임에서, 블록체인 패러다임으로 전환 중

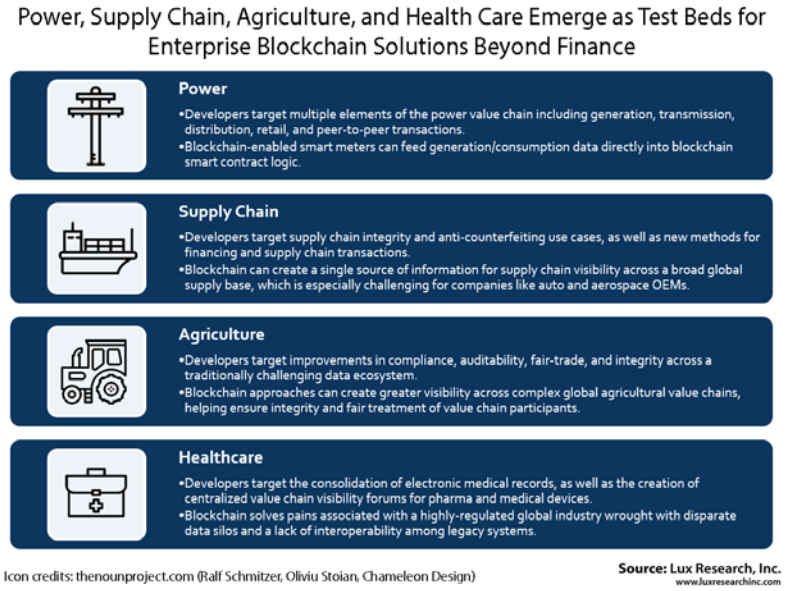
다수의 컴퓨터가 **중앙 신뢰기관 없이** 미리 합의된 규칙에 의해 공동의 작업을 수행하며(신뢰보장, 공증효과), **데이터가** 중앙서버에 집중되지 않고 **모든 컴퓨터 (노드)에 공유**되는 **탈중앙 비즈니스 (투명성, 익명성)**

중앙 집중 비즈니스 ➔ 탈중앙화 P2P 비즈니스 패러다임 전환

2018 블록체인 트렌드 (1)

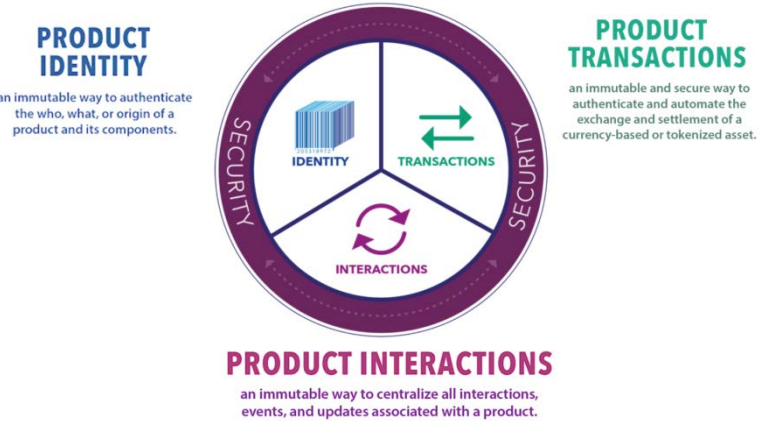
금융 이외의 분야로의 확산

- 블록체인이 **금융** 뿐만 아니라 거래 기록을 감독할 필요가 있는 모든 분야에 적용이 가능하고 유용하다.
- IDC 보고서는 2020년까지 **의료분야**에 20%가 블록체인 기술을 도입할 것으로 예측
- **인사관리**(이력서 위조방지), **법률분야**(등기 위조방지) 등의 분야에 대표적으로 사용될 수 있을 것



IoT 디바이스와 융합

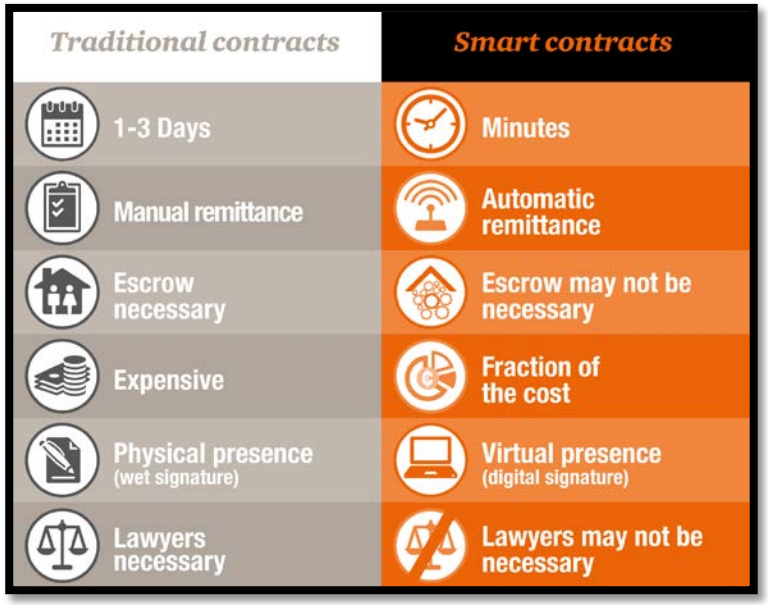
- 산업분야 및 가정에서 **사물 디바이스(IoT)**에 연결된 인트라넷 또는 인터넷 망에 활용될 수 있다.
- 디바이스 수가 증가하면서 이를 효율적이고 안전하게 관리하는 수단으로 블록체인을 고려해 볼 수 있다.
- M2M 에도 **사물 간 결제 및 거래**에도 활용할 수 있을 것으로 예측



2018 블록체인 트렌드 (2)

스마트 계약

- **Ethereum 2 세대 암호화폐** 플랫폼부터 등장한 스마트 계약 시스템은 *계약 조건이 충족되면 자동으로 계약이 체결된다.*
- 스마트 계약 방식은 다양한 산업 분야에서 활용될 수 있을 것으로 전망된다.
- 예를 들면 직원의 KPI 성과가 일정 수준을 달성하면 자동으로 성과급이 지급되는 것



국가공인 암호화폐 등장

- 암호화폐에 대한 각국 정부의 시각은 대체로 좋지 않은 편이지만, 일부 국가에서는 긍정적인 면을 부각시킴
- 블록체인의 긍정적인 효과를 바라보는 일부 정부에서는 암호화폐 제작을 공언하고 실제 개발 중
- 암호화폐의 **투기적 변동성**에 의한 부정적 효과도 있어 암호화폐로서의 블록체인 기술의 미래는 **불투명**

블록체인 기술적용 분야

블록체인 비즈니스 응용사례

금융 은행 (해외) 분야
글로벌 중앙 은행들이 자체 암호화폐를 개발하거나 블록체인을 금융 프로세스에 도입

금융 은행 (국내) 분야
블록체인을 직접 활용한 비즈니스보다는 해외송금, 인증과 같은 서비스에 활용

기업 투자 분야
크라우드 펀딩으로 기업에 투자할 수 있는 ICO 와 같이 신규자금 확보 수단에 활용

물류/유통 분야
다양한 회사가 관여하는 여러 단계의 복잡한 계약의 서류 기록을 간소화하고 위변조 가능성을 차단하는데 블록체인 기술이 적극 활용

의료 분야
환자의 개인건강기록 관리에 블록체인 기술을 적용하여 환자가 직접 본인의 의료정보를 관리

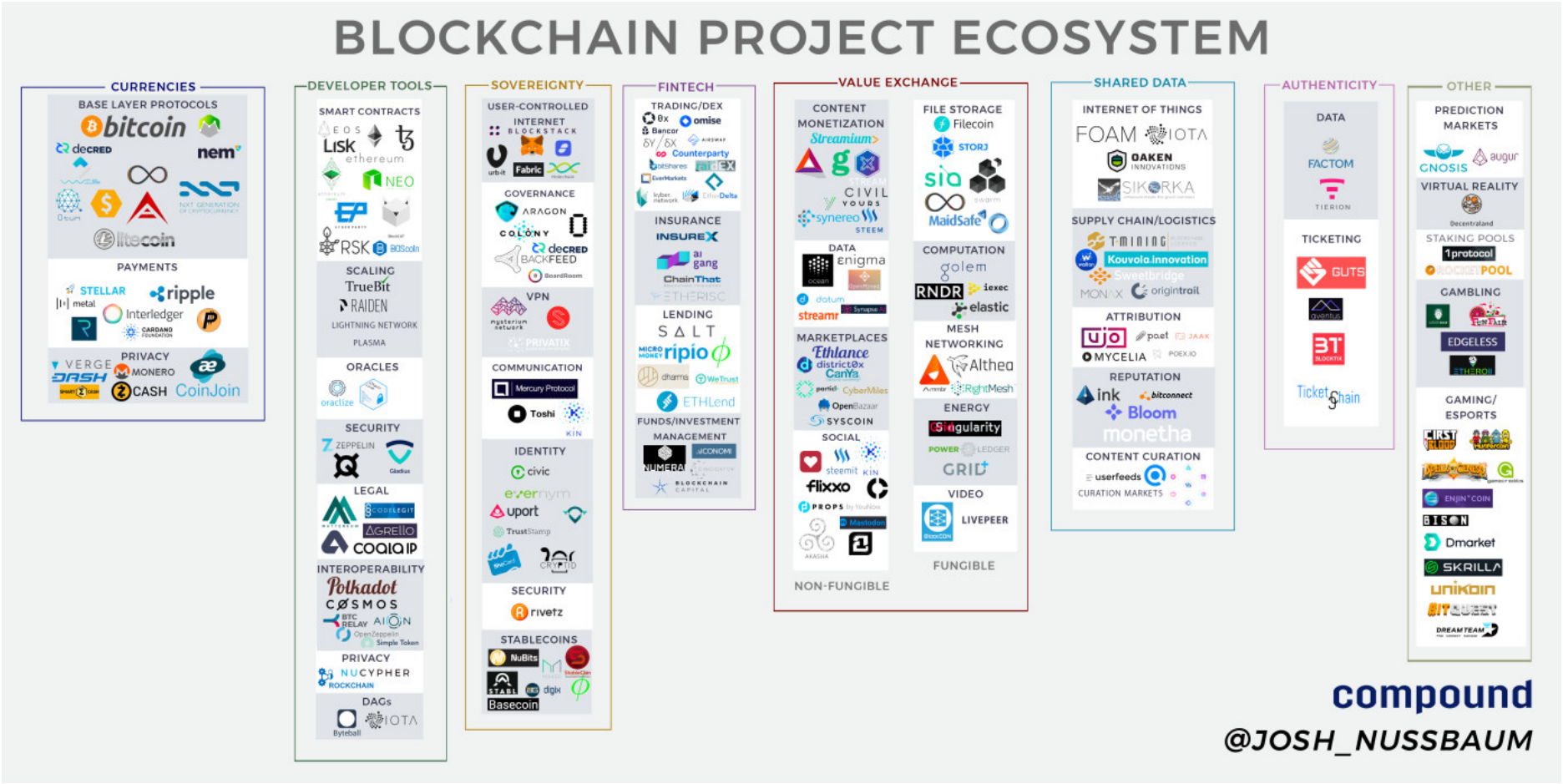
에너지 분야
에너지 생산·분배·거래를 위한 스마트그리드에 블록체인 기술을 적용함으로써 시장을 확장하고 효율화

공공서비스 분야
법·규제의 집행과 복지 서비스의 효율성 제고 등을 위한 블록체인의 활용이 적극적으로 시도

블록체인은 다양한 산업 영역으로 응용하여 신시장 창출

블록체인 기반 프로젝트 생태계

- 전 세계에 수많은 블록체인 적용 프로젝트가 진행중으로, **통화, 개발자 도구, 핀테크, 주권, 가치 교환, 데이터 공유, 진정성**의 분류
- 현재 블록체인 기술, 암호화된 화폐, 그리고 토큰 판매가 굉장한 붐이며, 이더리움의 대두와 함께 스마트 계약이 새로운 트렌드 형성
- 블록체인 **개념 검증**을 위한 시기를 벗어나 실생활에 적용하여 **소비자 경험 향상**을 위한 프로젝트가 활발히 진행 중



Source: https://medium.com/@josh_nussbaum/blockchain-project-ecosystem-8940ababaf27

블록체인과 금융산업

- 금융기관들은 블록체인을 통한 비용 절감, 효율성 제고를 목표로 **자체 프라이빗 블록체인** 또는 컨소시엄 참여를 통해 **생태계 구축**과 **서비스 표준화**를 시도 중
- 블록체인은 주식투자 또는 크라우드펀딩(crowdfunding) 등 기업에 대한 투자에도 활용될 수 있으며, 대표적인 예시로는 **ICO(Initial Coin Offering)**가 있음

금융 분야 적용 사례

증권, 거래
블록체인 기반의 거래 플랫폼을 제공하고, 스마트계약 기능을 이용하여 효율성을 높이도록 시스템을 개발 중

청산, 결제, 송금
정부의 감사, 규제 내에서 거래를 관리할 수 있도록 하며, 다양한 통화와 가상화폐를 이용할 수 있는 메커니즘, 플랫폼 개발 진행 중

투자, 대출
투자자(벤처캐피탈, 엔젤투자, 크라우드 펀딩, 개인 등)와 스타트업 기업을 연결시켜 투자금을 확보하기 위한 플랫폼 제공

상품 거래소
블록체인 기반의 거래 플랫폼을 통해 자산과 금융상품 거래가 가능하도록 기능을 제공하며, 이용 가능한 가상화폐를 지속적으로 추가

무역 금융
무역거래 시 이용되는 문서(계약서, 신용장 등)의 위변조 방지, 처리절차 간소화 등에 적용

금융분야 적용사례

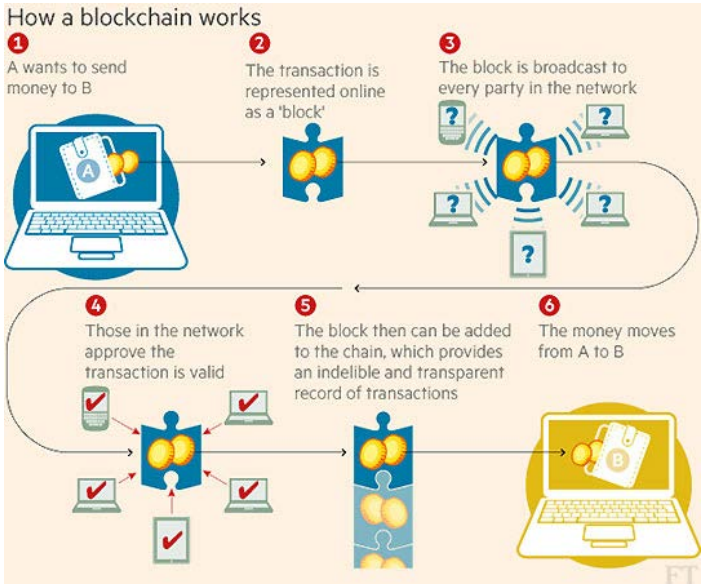
- 해외 은행들은 **직접 블록체인 R&D에 참여**하여 **암호화폐를 개발**하거나 **콘소시엄 블록체인**을 **금융 프로세스에 도입**
- 국내 은행들은 블록체인을 직접 활용한 비즈니스보다는 **해외송금·인증과** 같은 서비스에 블록 체인 기술을 적용하고 있음

① (국내) KB 국민카드

- KB국민카드는 2015년부터 카드의 적립 포인트를 가상화폐(비트코인)로 전환하는 서비스에 블록체인 기술 도입
- KB국민카드는 금융권 최초로 앱 카드인 'K-모션'에 블록체인 기술을 적용하여 공인인증서가 필요 없는 블록체인 기반의 간편인증 서비스 제공

→ *간편인증 서비스로 사용자 편의성을 제고하고 프라이빗 블록체인을활용하여 보안 및 신뢰성도 강화*

② (해외) 미국 나스닥 및 ICO 자금 모집



- 미국 나스닥은 블록체인 상에서 디지털 형태의 주식을 발행할 수 있는 링크(Linq) 시스템을 구축하여 2015년 말 첫 주식 발행에 성공
- ICO는 기업공개(IPO)와 유사하지만 토큰이 기업의 지분이 아니라 향후 서비스에 이용이 가능한 자원이라는 차이점이 있으며, 일반 개인투자자 대상의 크라우드펀딩 진행이 용이

→ *주식투자 또는 크라우드펀딩(crowdfunding) 등 기업에 대한 투자에도 활용*

블록체인과 의료산업

- 환자의 개인건강기록 관리에 블록체인 기술을 적용하여 환자가 직접 본인의 의료정보를 관리할 수 있게 하는 프로젝트가 추진 중
- 환자는 블록체인 상의 본인의 의료기록을 조회할 수 있는 개인키를 의사에게 안전하게 전달하고, 스마트계약을 통해 미리 정해진 기간 동안만 열람하도록 설정할 수 있음

의료 분야 적용 사례

IBM 왓슨헬스

미국 질병관리예방센터와 협력하여 기존에 병원이 보유한 진료 정보를 블록체인 네트워크에 저장하고 사물인터넷 등을 접목

IBM Watson

에스토니아 정부

국민의 의료정보(진료기록)를 블록체인 상의 개인 계정을 통해 관리

메디블록

의료정보의 관리·유통을 위한 퀀텀 블록체인 상의 분산어플리케이션을 개발 중

MEDIBLOC

밀의료 병원정보시스템

블록체인을 적용하여 의료데이터 접근권한 통합관리, 과금체계 기반 구축, 공인인증서 대체기술 개발을 추진

의료분야 적용사례

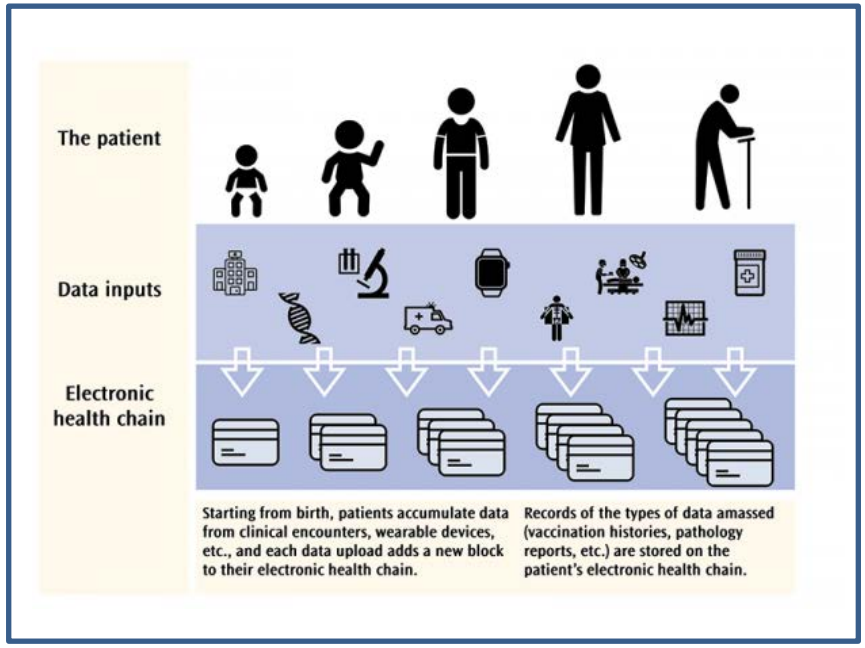
- 헬스케어 데이터를 안전하게 수집 (**암호화된 의료 데이터를 블록체인에 저장 및 관리**) 및 거래할 수 있게 하여 병원, 연구기관, 기업 등에는 진료나 연구, 헬스케어 관련 상품 개발에 도움 되는 데이터를 제공하고 개인에게는 자신의 데이터를 **열람 및 제어(데이터 통제권 부여)**하고 공유대상 업체를 선택할 수 있도록 모델을 설계 함

① (국내) 메디블록

- 환자의 진료기록은 수기로 작성되거나 병원마다 개별적으로 저장되어 진료 기록 조작 가능성, 환자의 불편 및 의료비 증가 등의 문제가 발생
- 병원에서 의사가 개인의료 정보를 기록하면 블록체인 플랫폼에 암호화 저장이 되어 복호화 키를 가진 본인만 열람·거래가 가능

→ *환자 중심의 통합 의료정보 관리가 가능하며, 의료정보 교류의 확대와함께 병원 간 유기적 협력할 수 있는 기반 마련*

② (해외) 보건정보기술국



- 건강데이터는 진료기록, 유전체 정보, IoT 기기에서 수집되는 라이프로그 방식의 민감정보로 중앙집중식 관리에 따른 비용·책임 가중
- 암호화된 건강데이터는 '데이터 호수(Data Lake)'에 저장되고 '의료기록소(Health Records)'가 사용자의 고유식별자와 함께 '헬스 블록체인'에 저장·관리

→ *개인의건강데이터주권을인정함과동시에 이해관계자간 안전한데이터 활용체계를 구현하여 의료 부가가치 창출에 기여*

블록체인과 물류/유통산업

- 다양한 회사가 관여하는 여러 단계의 복잡한 계약의 서류 기록을 간소화하고 위변조 가능성을 차단(투명성 제고)하는데 블록체인 기술이 적극 활용
- 블록체인 상에서 사물인터넷 센서를 통한 물류·유통의 전 과정의 투명한 모니터링을 통해 중간 과정의 문제 발생 시 책임 소재를 명확히 밝힐 수 있음

물류/유통 분야 적용 사례

UPS, 머스크

미국 UPS는 블록체인트럭운송협의체에 합류하여 표준화에 주력할 것을 발표, 해운회사 머스크는 컨테이너 화물 추적 시스템에 하이퍼레저 패브릭을 적용

글로벌 식품 기업

월마트등 8개 글로벌 식품 기업은 IBM과 협력하여 식품의 유통 전과정에 블록체인을 적용하여 투명성과 신뢰성을 확보할 계획

관세청

관세청은 블록체인 컨소시엄 시범사업을 통하여 수출통관 업무(수출 신고 및 적하목록 제출 절차)에 블록체인을 적용 타당성 검증

SK C&C

SKT의 사물인터넷 전용망 로라(LoRa) 망을 활용해 블록체인 기반 컨테이너 화물 추적·관리체계를 구현하고, 한국-상하이 구간의 컨테이너 화물을 대상으로 시험을 수행

현대상선

냉동 컨테이너 시험항차(한국-중국) 및 인도·중동·유럽 항로 컨테이너선 시험운항을 완료

물류/유통분야 적용사례

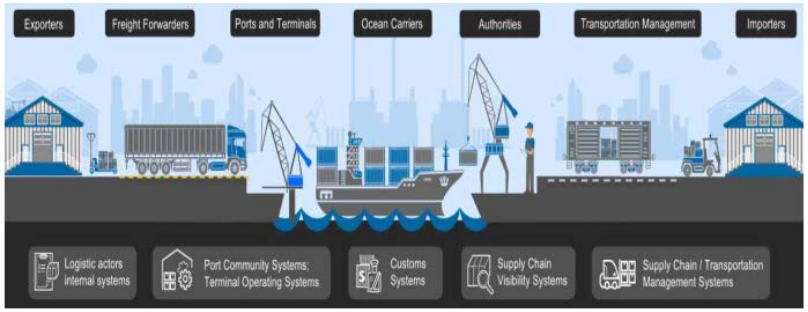
- 해외는 업계의 주요 기업들이 IT기업과의 협력 및 블록체인 관련 협의체 구성을 통해 물류· 유통업계에 블록체인을 도입하는 작업에 착수하였으며, 2018년 1월 세계 최초 블록체인을 이용한 대규모 농산물 국제 거래가 완료됨

① (해외) 식품안전망 솔루션

- 특정 제품의 문제가 어디서 발생하였는지 신속하게 감지함으로써 오염된 음식을 통해 발생하는 피해와 질병을 예방
- 월마트(Walmart) 돼지고기 유통과정에서 발생하는 주요 데이터를 입력·저장·공유할 수 있도록 블록체인 기반 플랫폼 개발

→ *소비자는 안전한 먹거리 유통을 보장받을 수 있고, 공급자는 소비자에게 신뢰를 구축하여 브랜드 이미지 강화*

② (해외) 스마트계약 기반의 물류운송 추적시스템



- 종이문서에 의한 거래계약·확인 의존도가 높아 시간.비용 등의 비효율 초래
- 상품의 전 무역거래 과정(문서 제출·확인·승인 등)이 디지털화된 자동화 방식으로 처리되도록 블록체인의 스마트계약이 적용

→ *실시간으로 운송 정보를 확인할 수 있어 공급망의 가시성을 제고하고궁극적으로 통관과 화물 이동에 걸리는 시간과 비용을 절감*

블록체인과 에너지산업

- 에너지 생산·분배·거래를 위한 **스마트그리드 및 마이크로그리드**에 블록체인 기술을 적용함으로써 시장을 확장하고 효율화
- 지역기반 **신재생에너지 생산·거래 플랫폼, 전기차 충전 시스템** 등의 비즈니스 모델이 개발

에너지 분야 적용 사례

전력 거래

에너지 생산(공급)자가 중개사업자 없이 자신이 소비하고 남은 에너지의 판매가 가능하며, 암호화폐를 통한 전력요금 결제, P2P 에너지 거래

스마트그리드(smart grid)는 기존의 전력망에 IT기술을 접목하여 에너지 생산(공급)자와 소비자가 실시간으로 정보를 교환하고 전력을 거래하는 지능형 전력망을 말하며, **마이크로그리드**(micro grid)는 생산(공급)자와 소비자의 위치가 가까운 국소 전력공급시스템을 뜻함

솔라코인(Solar Coin)

신재생 에너지 생산에 따른 보상체계로서, 태양광 발전량에 따라 암호화폐를 지급하여 패널 시설 보급을 장려

독일의 RWE

블록체인 기반의 전기차 충전 지불 시스템 블록차지 (BlockCharge) 프로젝트를 추진

한국전력

블록체인 기반 이웃간 전력거래 및 전기차 충전 서비스를 구축

블록체인 기반 전력거래 플랫폼을 구축하여 실시간으로 잉여전력 판매자와 소비자를 연결하고, 블록체인을 기반으로 전기차 충전소 데이터 관리, 충전 서비스 대외업무처리, 충전 이용 고객 지원 서비스 등을 통합

브루클린 마이크로그리드

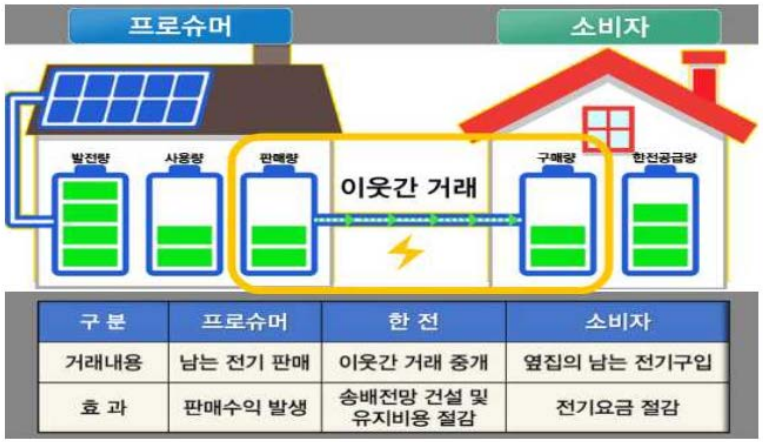
지역 건물 간 전력거래 플랫폼
- 지역 주민들이 전기수요를 충족하기 위해 개인이나 집단 단위로 참여

에너지분야 적용사례

- 해외의 경우 미국, 유럽을 중심으로 **지역기반 신재생에너지 생산·거래 플랫폼, 전기차 충전 시스템** 등의 비즈니스 모델이 개발 중

① (국내) 한국전력공사

〈 블록체인 기술을 적용한 사용자(프로슈머-소비자)간 전력거래 구상도 〉



구 분	프로슈머	한 전	소비자
거래내용	남는 전기 판매	이웃간 거래 중개	옆집의 남는 전기구입
효 과	판매수익 발생	송배전망 건설 및 유지비용 절감	전기요금 절감

- 공급자-수요자 간 신속한 매칭이 어렵고 실시간 거래가 어려워 이를 보완하기 위해 도입
- 전력거래는 '에너지포인트'로 이루어지고 보유한 포인트는 전기요금 납부 외에도 현금 환급, 전기차 충전소에서 사용 가능

→ *블록체인의 탈중개성 등을 바탕으로 이웃 간 전력거래 서비스가 확산되어 손쉽게 전력을 거래하고, 전기요금 부담이 완화*

② (해외) 솔라 코인

- 신재생 에너지 생산에 따른 보상체계로서, 태양광 발전량에 따라 암호화폐를 지급하여 패널 시설 보급을 장려
- 1 솔라코인이 1,500파운드(약 680kg) 수준의 이산화탄소 배출 감축효과

→ *재생에너와 관련한 새로운 가치 창출의 기회 확보뿐 아니라 다방면의 비용절감 효과도 기대*

블록체인과 공공서비스산업

- 공공 부문에서는 **법·규제의 집행과 복지 서비스의 효율성 제고** 등을 위한 블록 체인의 활용이 적극적으로 시도되고 있음
- 공공 데이터를 개방·공유하고 국민 개개인의 편익을 위한 양방향 맞춤형 서비스를 제공하는 **정부 3.0 패러다임**에 부합하며, 공공부분에서 큰 역할을 할 수 있을 것으로 기대

전자투표

전자투표의 조작(해킹)방지 및 투명성(신뢰성)을 위해 국내외 정당과 지자체를 중심으로 블록체인의 적용이 시도되고 있음

- **스페인**의 정당 포데모스(Podemos)와 **호주**의 정당 플럭스(Flux)는 정당 내의 의견수렴에 **블록체인 기반의 전자투표** 방식을 활용하고 있으며, **미국** 공화당과 자유당은 대선후보 경선에 블록체인 기반 전자투표를 이용한 바 있음
- **우크라이나** 정부는 청원 및 자문 투표를 위한 **블록체인 활용 선거 플랫폼** 사용 계획을 발표

부동산관리

미국, 스웨덴, 조지아공화국 등은 부동산 등기와 거래에 블록체인을 적용하는 시범사업을 추진 중

- **미국 버몬트주**는 **부동산 거래기록 관리**에 블록체인을 도입하는 시범사업 추진
- **스웨덴 국토조사국**은 **토지 관리시스템**에 스마트계약을 적용하여 토지 거래자, 부동산 중개인, 은행 등을 연결하는 서비스를 개발하여 평균 3개월이 소요되는 거래 프로세스를 수일 수준으로 단축할 것으로 기대
- **조지아공화국**은 **부동산 소유권·계약 위변조를 방지**하기 위해 공공 등기청의 국가 토지대장관리를 블록체인 방식으로 전환하는 프로젝트를 추진 중

복지

복지 수당 지급의 효율성과 투명성 제고를 위해 블록체인 도입이 추진 중

- 영국의 **거브코인**(GovCoin)은 바클레이즈 은행, 런던대학교 등과 협력하여 **노동연금에 블록체인을 결합**한 공공복지 시스템을 개발 중
- **서울시**는 **청년수당 지급 과정**에 블록체인 기술을 적용하여 서류 발급 확인 절차를 간소화하는 등의 공공복지 서비스를 개발 중

기록,관리

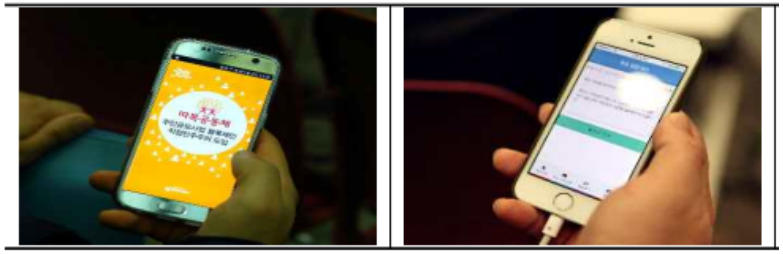
디지털증거보존, 활용체계(영국), 전자문서 기록, 관리 시스템(두바이)

공공서비스분야 적용사례

- 전자투표의 조작(해킹)방지 및 투명성(신뢰성)을 위해 국내외 정당과 지자체를 중심으로 블록체인의 적용이 시도되고 있음
- 블록체인 기반의 가상화폐를 지역화폐로 활용하여 사용편의성을 제고하고 지역화폐 이용의 활성화 도모

① (국내) 따복공동체 주민결정을 위한 전자투표

〈 따복공동체 앱 〉 〈 따복공동체 번호확인 〉



- 주민투표 참여율을 높이고 다수 국민의 의견을 반영한 정책결정을 위해 선제적으로 도입
- 투표할 공동체 번호를 확인한 후, 따복공동체 앱에 미리 배부된 투표권 QR 코드를 인식하고 공동체 발표영상을 보며 앱으로 투표

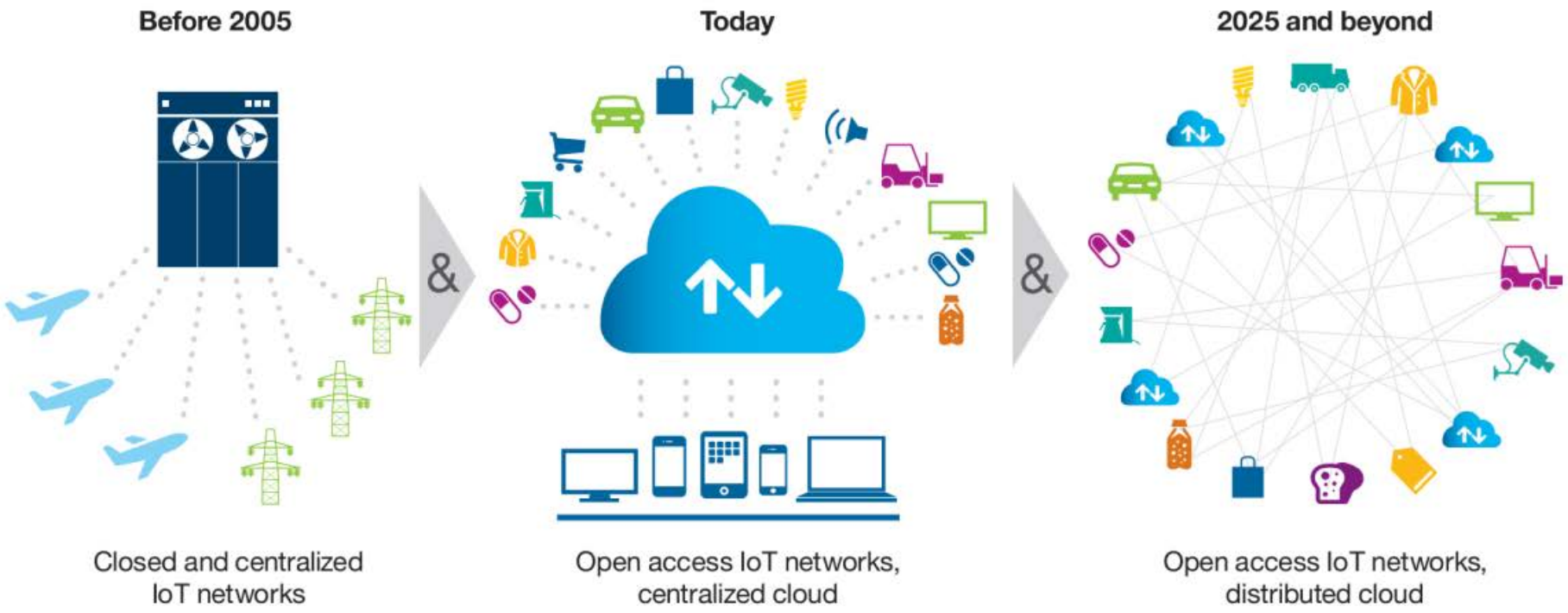
→ QR코드에 블록체인 기술이 도입되어 심사시작 전까지 불법조작이 불가하기 때문에 투표의 투명성·객관성·신뢰성 등 제고

② (국내) 지역기반의 가상화폐 '노원(No-Won)

- 블록체인 기반의 가상화폐를 지역화폐로 활용하여 사용편의성을 제고하고 지역화폐 이용의 활성화 도모
- 노원은 '앱'과 '카드'의 QR코드를 통해 노원가맹점 총 122개(공공21개소, 민간 101개소) 화폐처럼 사용할 수 있고, 사용자 간 거래 (선물)도 가능

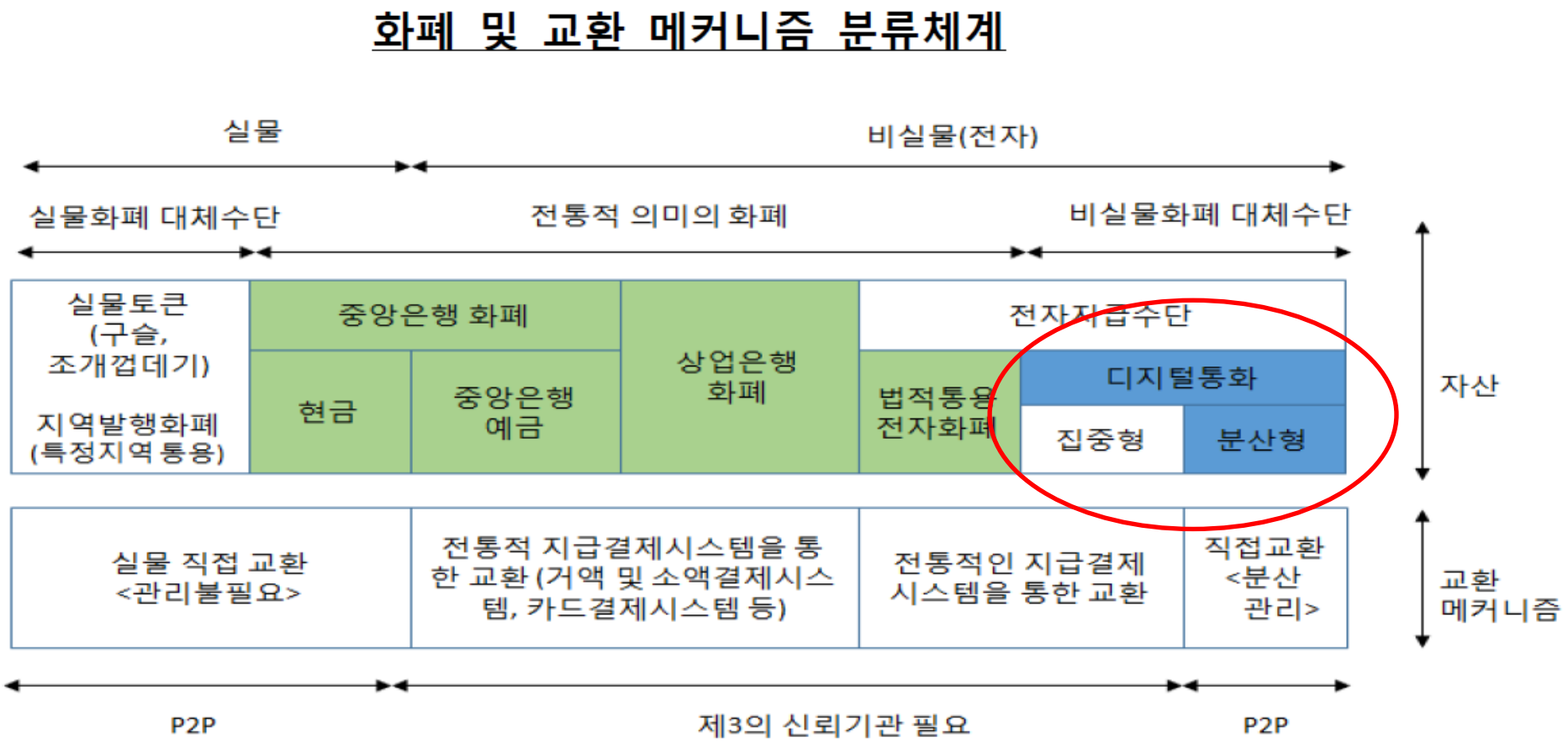
→ 거래 내용이 투명하고 안전하게 공개되는 블록체인 기술과 시장가치로 반영되지 않는 사회적 가치가 결합한 실증사업의 모범예시로 확산

"SILO화 된 것은 집중화 되고, 집중화 된 것은 가상화를 거쳐 결국 분산화 된다."



- 통신 : CDMA/W-CDMA/LTE → 집중화 및 S/W화(가상화) CCC → D2D/ad-hoc/Mesh
- IDC : 개별 서버와 스토리지 → Cloud IDC → P2P/Distributed Computing
- 공유경제 : 택시산업 → 중앙Platform화(Uber) → dApp을 통한 LaZooz의 Zooz Token
- 회사: 주식회사형 창업 → 규모화를 위한 IPO → ICO를 통한 프로토콜(규약) 형태 창업

암호화폐의 위치



자료: BIS(2015)

화폐의 중앙화 → 가상화 → 그리고 분산화?

화폐의 중앙화 → 가상화 → 분산화 과정

	현금 (중앙화)	전자화폐 (가상화)	암호화폐 (분산화)
발행 기관	중앙은행	금융 기관, 전자금융업자	없음 (DAO)
발행 규모	중앙은행 재량	법정통화와 1:1 교환	알고리즘에 의해 사전 결정
거래 기록 및 승인	불필요	발행기관 및 청산소	분산원장 이용 P2P 네트워크
화폐 단위	법정 통화	법정 통화와 동일	독자적인 화폐 단위 (BTC, ETH 등)
법정통화와 교환 여부	–	발행 기관이 교환을 보장	가능하나 보장되지 않음
법정통화와의 교환 가격	–	고정	수요–공급에 따라 변동
사용처	모든 거래	가맹점	참가자

출처: IBK기업은행경제연구소(2017.07) 도표를 인용 및 가공

탈중앙화(Decentralization)의 한계

문제점

블록체인의 탈중앙화 추구 이념에 따라 채굴자의 수, 노드 수, 블록 전송에 필요한 대역폭등의 확장성과 상충되는 문제점이 대두됨

- **유통의 구조적 한계 → 기하급수적 증가하는 거래 장부를 모든 노드에 동기화 시키는 과정에 따른 용량과 네트워크 부하가 증가**
- **채굴풀의 독점화 현상 → 비트코인 채굴 풀의 경우 3%가 총 연산 능력의 56%를 소유**
- **채굴 방식의 문제 → PoW 합의 알고리즘을 수행하는 과정에서 파생되는 문제점**

유통의 구조적 한계
- 발행만 고려한 구조적 설계 (비트코인)
- 노드 수의 기하급수적 증가
- 참여자 증가에 따른 장부의 크기가 기하급수적으로 증가 (년간 280GB 증가)

채굴 풀의 독점화
- 해킹에 의한 위험성(공격 대상이 적어짐)
- 소수 업자에 의해 집중(채굴장 대부분이 중국에 밀집 전체 해시율의 81%를 차지)
- 51% 공격 문제

보상 방식의 한계
- 채굴 참여에 대한 보상이 줄어듬
- 작은 거래에 대한 메인넷 서버 부담
- 채굴 난이도 계속 증가함에 따라 소비되는 전력 및 자원 낭비

개선 방안

새로운 알고리즘
- PoW 방식을 탈피
- 라이트코인, 이더리움, 이오스 등의 알트코인 등장
- 하드 포킹(UAHF), 소프트 포킹

합의 방식 개선
- PoS 및 분산합의 알고리즘 도입
- 커뮤니티 차원에서 민주적인 합의 및 감시
- 이용자의 의사 결정 참여 유도

서비스 본질 가치 창조
- 암호화폐 본질적 가치 보완(유통, 교환, 자산 등의 통화 가치 창출)
- 토큰의 서비스 가치 창출(서비스 유지 동인으로서의 역할 보완)

비트코인 탈중앙화 한계로 부터 블록체인 비즈니스 적용에도 유사한 문제해결방안 모색가능

중앙집중 거래소 문제

문제점

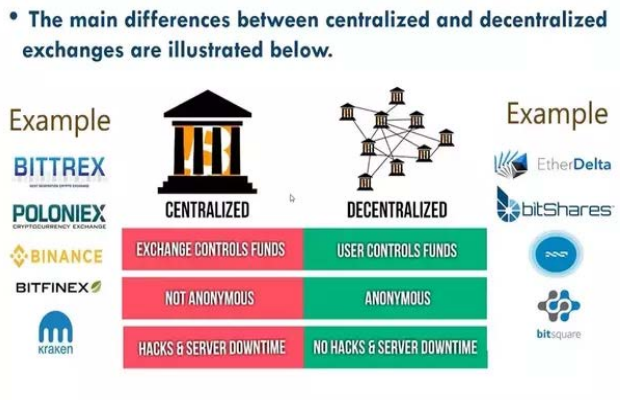
- 암호화폐가 통화 유동성을 확보하기 위한 방안으로 암호화폐 거래소가 등장 (익명성이 사라짐)
- 투기적 요소를 조장하고 시스템을 중앙집중화 시키면서 빈번한 해킹 및 개인정보 유출 우려를 낳으며 탈중앙화의 본질적 가치와 오히려 상반된 결과를 낳게 됨

중앙집중식 거래소
- 해킹에 의한 위험성 (보안 취약성)
- 거래소의 서버다운(service continuity) 위험
- 법적 보상체계 미흡(지급보증 의무 부재)
- 자산의 **보관 역할**을 대신함 (위험도증가)
- 신뢰적 보안 인증 절차 미흡
- 규제(compliance) 일관성부재 (신뢰문제)

개선 방안

탈중앙화 거래소
- 모든 자산을 개인이 보관 (하드웨어 지갑 제공) 또는 신뢰할 수 있는 대리 보관
- 중개인 없는 개인간 거래 (P2P Exchange)
- FIDO U2F1 지원 (인증 강화)
- 법정화폐의 교환을 위해서는 하이브리드 방식을 사용하기도 함 (중개 역할 분리)
- 교환 역할에만 충실

◇ [그래픽=아이뉴스24 DB]



중앙 집중 암호화폐 거래소 ➔ 탈중앙화 P2P 암호화폐 거래소 전환

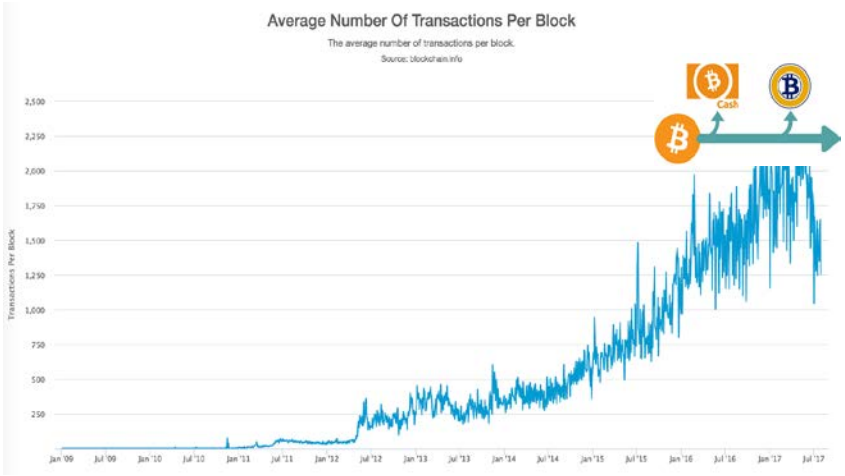
제한된 확장성 (Limited Scalability) 문제

문제점

- **신규거래가 발생할 때마다 추가되는 블록들이 모두 체인으로 엮이면서 시간이 갈수록 기하급수적으로 늘어나는 거래 장부를 모든 노드에 재전송하여 동기화 시켜야 하므로 갈수록 용량과 네트워크 부하가 증가할 수밖에 없는 구조**

처리 속도 한계
- 처리 가능 거래 숫자는 초당 최대 7건
- 병목 현상에 의한 잦은 지연 발생
- 블록 사이즈의 제한 (1MB) 에 의한 거래 처리 속도에 한계

높아진 거래 비용
- 거래인증/채굴에 사용되는 컴퓨터들은 네트워크 비용 및 상당한 전기료까지 부담
- 지속적 채굴 난이도 상승에 의한 채굴자의 투입 비용이 증가하여 거래 처리 비용이 상승하게 됨



Source: https://blockchain.info/charts/market-price?timespan=all and https://blockchain.info/charts/cost-per-transaction?timespan=all

비트코인 설계의 태생적 한계성 ➔ 합의 알고리즘 개선 (채굴 방식 전환)

막대한 채굴 에너지 소비문제

문제점

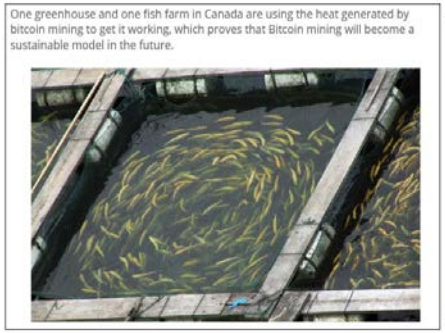
- **채굴의 난이도 상승에 의해 하드웨어가 계속해서 업그래이드 되어야 새로운 신규 토큰을 일정하게 보상 받을수 있음**
- **채굴 난이도가 증가하면 에너지 요구량도 그에 비례해 증가**

에너지 낭비

- 블록체인 방식은 다수 개인들의 거래인증 참여를 통해서만 유지가 가능한데, 거래인증/채굴에 사용되는 컴퓨터들은 네트워크 비용에다 상당한 전기료까지 부담을 해야 함
- 비트코인 채굴은 159개 국가보다 더 많은 전기를 소비

생산적 에너지로 전용

- 캐나다의 일부 온실안의 물고기 양식장에서 비트코인 채굴 시 발생한 열 에너지를 이용하여 운영하는 사례가 있음
- 채굴 시 발생하는 열 에너지를 이용한 히터기 제품 개발 시도



비트코인 채굴에 따른 과도한 에너지 소비 → 발전적 시스템에 전용

Conclusion

어떤 모델에 블록체인을 도입해야 하는가?

블록체인 기술은 탈중앙화(decentralization) 측면과 확장성(scalability)의 균형(trade-off)을 고려하여 도입해야 함
→ 적용대상의 선별적 도입 후 검증 후 점진적 개선 및 확대 적용 방식으로 도입하는 것이 바람직

핵심 요소

충분한 가치(value)
(블록체인을 유지할 수 있는 충분한 유인 가치가 존재해야 함)

익명성(transparency)
(참여자가 투명하게 노출되어 악용방지,개인정보 보호 필요성)

거래량(Transactions)
(블록체인 노드 증가에 따른 확장성의 제한 및 처리속도 고려)

신뢰 문제(trust)
(보안성, 투명성이 중요한 사례의 경우 –중간관리기구 신뢰도 낮음)

데이터(database)
(모든 노드에 보안적으로 안전한 데이터베이스가 필요한지 여부)

수익구조 고민
- **탈중앙화**는 인프라구축비용 및 **거래 수수료 절감** 효과
- 코인의 화폐가격이 미래에 일정하다 하더라도 참여자들에게 수익성을 보장
- 투기적 수요에 의한 가치 상승이 아닌 비즈니스 본연의 수익 원천이 존재해야 함

탈중앙화(투명성/보안성/변경불가)

- 내용 수정이 불가능한 구조(immutable) ← → 잊혀질권리
- 탈중앙화 ← → 약한 체인 (보안 취약성의 확산)
- 투명성 ← → 프라이버시 침해

확장성(처리속도/저장공간)

- 시간당 거래 처리속도가 제한적 (대량 거래 구현 어려움)
- 저장 공간이 점점 증가 (장기적으로 용량 이슈 발생)
- 허가형(private)블록체인 고려

Conclusion

블록체인 성공적 도입을 위한 5가지 핵심 요소

Key Factors

블록체인은 데이터베이스가 아닌 네트워크이다

분산 데이터베이스는 데이터를 공유하기 위한 시스템 도구인 반면 블록체인은 변조가 불가능한 분산 장부 시스템으로서 B2B 시스템의 데이터베이스를 대체를 위한 것이 아닌 새로운 패러다임을 적용하기 위한 프레임워크로 접근해야 한다.

사용 시나리오를 명확히 정의하라

사용시나리오, 네트워크 참여자, 토큰의 가치 등을 명확히 정립해야 한다. 인프라 구축 후 모델을 계획하는 경우 개인정보보호, 컴플라이언스, 확장성, 성능이슈 등의 제한에 실패할 확률이 크다. 블록체인 유지를 위한 인센티브(사업 가치 요소, 수익화)를 실제 사업과 관련하여 수치화 시키는 작업이 필요

성능(throughput)과 확장성(scalability)

블록체인은 합의 알고리즘, 구현 모델에 따라 수백~수천 TPS 성능을 보여줄 수 있다. 사업 모델이 수백만 TPS 성능을 요구하는 경우 적용하지 말아야 한다. 또한 노드 수의 증가에 따른 확장성을 고려해야 하는데, 개발 과정에서 보인 성능과 확장 후의 성능에 차이가 발생할 수 있음을 인지해야 한다.

작지만 충분한 범위를 충족할 데이터

블록에 담길 데이터(거래,헬스케어 등)는 블록체인을 따라 외부 경계에 노출되어 기밀성,무결성,가용성이 문제 될 수 있다. 용량이 큰 데이터는 메인넷의 성능을 떨어뜨릴 수 있어 노드에 참조형으로 설계하거나 민감한 데이터는 규제(compliance)의 준수를 위한 최선의 방안을 설계 단계 부터 고려해야 한다.

자주 변하지 않는 데이터

블록에 담길 데이터는 장부(ledger)에 한 번 기록되면 삭제되지 않는다. 사용 시나리오가 자주 변경되는 데이터를 다루는 경우 다시 생각해 봐야 한다. 불가피할 경우 새로운 블록을 생성하여 업데이트, 삭제 할 수 있는 회피 방안을 설계해 볼 수 있지만 바람직 하지 않은 경우가 많을 것이다.

혁신은 암호화폐? 아니면 블록체인?

"암호화폐가 가지는 가장 파괴적인 특징은 이 기술로 경제 시스템을 프로그래밍 할 수 있다는 것이다. 인류는 최초로 다양한 경제 시스템들을 마음대로 실험해 볼 수 있는 시대에 도달했다." – **전명산 블록체인OS사 CSO**

➔ 암호화폐 : 자산, 화폐, 주식의 성격을 모두 가지고 있음. 설계한 원리의 위변조 불가능성

"암호화폐는 블록체인 생태계를 돌아가게 만드는 피, 프라이빗 블록체인은 허가 받은 소수만 참여할 수 있는 특정집단의 인트라넷에 불과. ICO는 젊은이들이 아이디어 하나만으로도 창업하고 돈을 그러모을 수 있는 제도인데, 탈중앙화 플랫폼을 키우겠다면서 피(암호화폐) 공급을 막는 꼴." – **최공필 금융연구원 미래금융연구센터장**

➔ 암호화폐 본질은 소통, 신뢰, 네트워크. 끊임없는 하드포크가 다양성 존중 생태계의 증거

"암호화폐의 과열된 에너지를 어떻게 활용할 것인가가 4차 산업혁명 시대를 준비하는 열쇠. 한국의 투자열기를 블록체인 기술개발과 비즈니스 부흥으로 연결시켜야." – **김서준 '크립토 펀드' 해시드 대표**

➔ 블록체인 기술은 좋지만 암호화폐는 위험하니 무조건적으로 제한해야 한다? 불가능한 이분법

"ICO 금지, 젊은이들 중 '제2의 이해진, 김정주'이 나오고, 또 이에 투자할 기회를 박탈하는 것. 자유경제에서 투자는 전적으로 개인의 책임이자 자유." – **전하진 (전)한글과컴퓨터 대표**

➔ ICO를 통해 창업자금을 모으고 서비스를 개발하는 기업인, 거래원장을 만들고 보관하는 채굴자, 암호화폐 투자자, 거래소, 이 모두가 필수불가결한 블록체인 생태계의 참여자들이다.

"블록체인은 암호화폐에 적용되는 수많은 기술들 중 하나일 뿐이며 암호화폐 빠진 블록체인은 무용지물. 많은 대기업들이 블록체인을 활용한 서비스를 제공할 것이다 하는데 이는 마케팅 차원의 쇼일 뿐, 실효성 없다 생각." – **김형중 고려대 정보보호대학원 교수**

"블록체인 자체는 서로를 믿지 못하는 거래 당사자들이 설치하는 값비싼 다중 분산형 DB에 불과" – **김연우 ㈜아홉 대표**

➔ 암호화폐가 혁신적인 이유는 정부가 만든 돈이 아님에도 전 세계의 많은 사람들이 실제로 암호화폐에 투자하고 있고 또 어떻게 이를 활용할 수 있을지 생각하고 있다는 그 자체.

➔ <세상을 바꾸는 혁신은 블록체인이 적용된 '암호화폐'이지 블록체인 기술자체가 아니다.>

감사합니다