

새로운 경제•사회•정치질서의 시작점으로서

블록체인과 사이버화폐

Youngwhan Lee, Ph. D.

C.P. 010-7997-0345

E-Mail nicklee@cha.ac.kr

Facebook Youngwhan Nick Lee

Twitter nicklee002



이름: 이영환 차대학 융합경영대학원교수

이메일: nicklee@cha.ac.kr

전화: 010-7997-0345

학력:

-1986.8 미국일리노이대학교 (어바나 샴페인)

수학과 전산학 공학학사 졸업.

-1991.2 미국일리노이대학교 (어바나 샴페인)

전산학 석사 졸업. (인공지능 전공)

-1995.10. 미국일리노이대학교 (어바나 샴페인)

전산학 박사 졸업. (인공지능 전공)

현 ISO/TC307 아이덴티티 연구반 의장

현 W3C 블록체인 커뮤니티 그룹 공동 의장

현 블록체인표준화포럼 의장

현 블록체인오픈포럼 표준화분과 분과장

현 공공데이터제공분쟁조정위원회 조정위원

현 데이터 거래 연구회 회장

현 한국강소기업진흥학회 수석부회장

현 한국데이터사이언스학회 전문이사

현 한국 금융ICT융합학회 부회장

현 차의과학대학교 융합경영대학원 부원장 겸 교수 (전 건국대 교수(2009년 3월 ~ 2017년 2월))

주요 업적:

- 앱 개발:

"발표채점," "폭력없는 우리학교," "제보자" 등 앱 다수 개발 배포 중

- 연구논문 및 보고서: (2016년 1.1. 이후)

1. 이영환, 전희주. "Nation Image and its Dynamic Changes in Wikipedia." APJIE. 2017, Jan.

2. 이영환. 국내외 블록체인 기술사례 및 적용분야 연구 보고서. 인터넷진흥원. 2016. 12. 31. KISA-WP-2016-0040.

3. 이영환, 오세경, 김재필, 권혁준. 분산원장 기술의 현황 및 주요 이슈 (1부 정책적 이슈). 한국은행 금융결제국. 2016. 12.

4. 이영환. "국가이미지 분석을 위한 위키피디아 실시간 동적 온톨로지 구축 알고리즘 및 적용." 한국데이터정보과학회. Jul. 2016. DOI : 10.7465/jkdi.2016.27.4.979.

- 저서: 웹3.0 세상을 바꾸고 있다. 보문각. (2010/06)

- 특허: 특허 제 10-1658199호. "데이터거래소에서 구독에 의한 데이터 거래시스템 및 그 방법" 외 2종

블록체인과 디지털화폐 혁명

비트코인 가격 폭등

Bitcoin Charts

Zoom 1d 7d 1m 3m 1y YTD ALL

From Apr 28, 2013 To Jul 2, 2017



Highcharts.com

출처: <https://coinmarketcap.com/currencies/bitcoin/>

이더리움 가격 폭등

Ethereum Charts

Zoom 1d 7d 1m 3m 1y YTD ALL

From Aug 7, 2015 To Jul 2, 2017



Highcharts.com

출처: <https://coinmarketcap.com/currencies/bitcoin/>

암호화폐(비트코인)의 시작

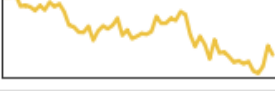
Bitcoin: A Peer-to-Peer Electronic Cash System

Satoshi Nakamoto
satoshin@gmx.com
www.bitcoin.org

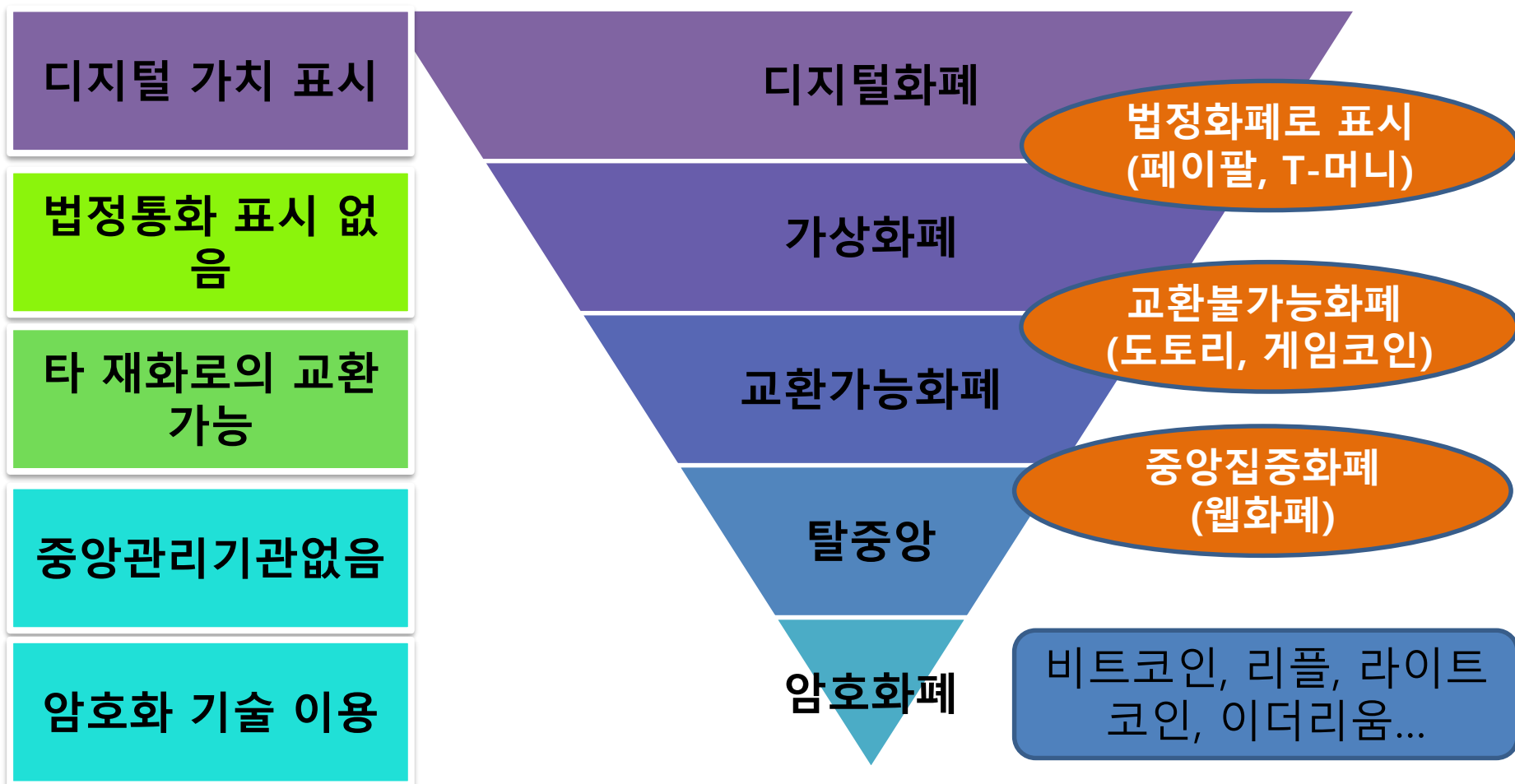
Abstract. A purely peer-to-peer version of electronic cash would allow online payments to be sent directly from one party to another without going through a financial institution. Digital signatures provide part of the solution, but the main benefits are lost if a trusted third party is still required 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.

2008년 세계 금융위기 이후 금융시스템에 대한 신뢰가 떨어지면서 사토시 나카모토라는 가명을 쓰는 발명자가 비트코인이라는 암호화폐를 고안함.

암호화폐

All ▾ Currencies ▾ Assets ▾ USD ▾ Next 100 → View All							
▲#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	 Bitcoin	\$18,733,542,568	\$1157.44	16,185,325 BTC	\$135,845,000	0.35%	
2	 Ethereum	\$1,215,282,661	\$13.62	89,247,460 ETH	\$14,437,400	0.06%	
3	 Ripple	\$211,864,376	\$0.005704	37,144,100,247 XRP *	\$356,616	0.67%	
4	 Dash	\$193,513,787	\$27.16	7,125,244 DASH	\$5,112,420	5.42%	
5	 Litecoin	\$191,077,085	\$3.83	49,954,532 LTC	\$2,879,780	-0.19%	
6	 Monero	\$167,935,555	\$11.98	14,017,525 XMR	\$2,646,000	-0.22%	
7	 Ethereum Classic	\$110,391,213	\$1.24	89,209,346 ETC	\$1,411,480	2.96%	
8	 MaidSafeCoin	\$78,284,326	\$0.172984	452,552,412 MAID *	\$583,801	0.82%	
9	 NEM	\$58,353,120	\$0.006484	8,999,999,999 XEM *	\$134,555	1.27%	

블록체인과 암호화폐



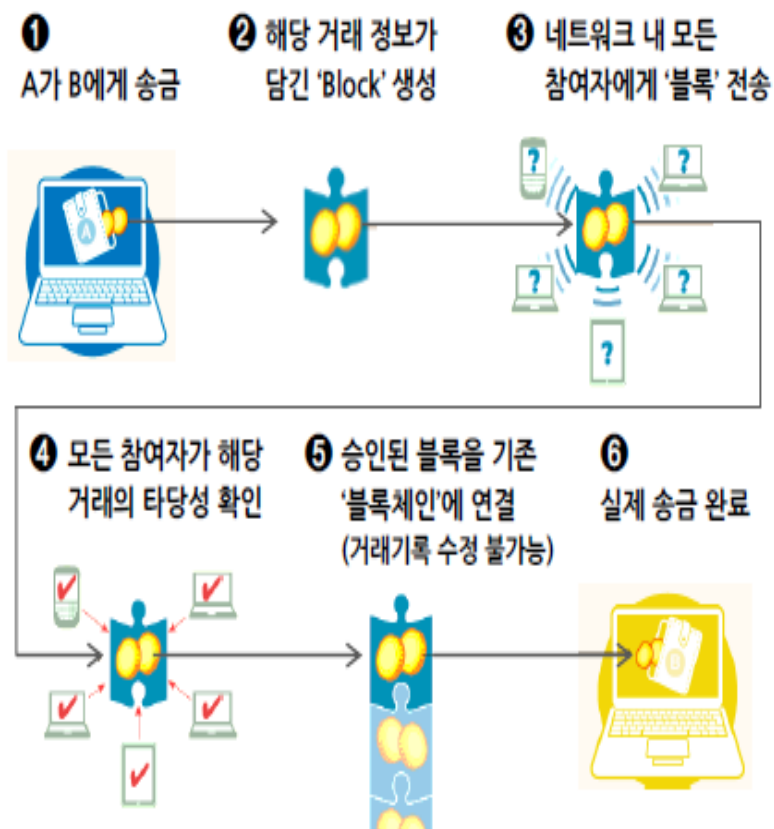
출처: He, Dong, Karl Habermeier, Ross Leckow, and Vikram Haksar. "Virtual Currencies and Beyond: Initial Consideration," International Monetary Fund, 2016.

블록체인이란?

- ▶ 밥 그라이필드 (나스닥 CEO)
 - 향후 십여 년 이상을 생각할 수 있는 가장 큰 기회
- ▶ 단 탭스콧
 - 소셜웹, 빅데이터, 클라우드, 로봇, 인공지능보다도 향후 십 년간 우리 사회를 더 많이 바꿀 기술
- ▶ 빌 게이츠
 - "A technological tour de force"
- ▶ 이영환
 - "모든 것의 신뢰제공 인프라(Trust infrastructure of everything)"

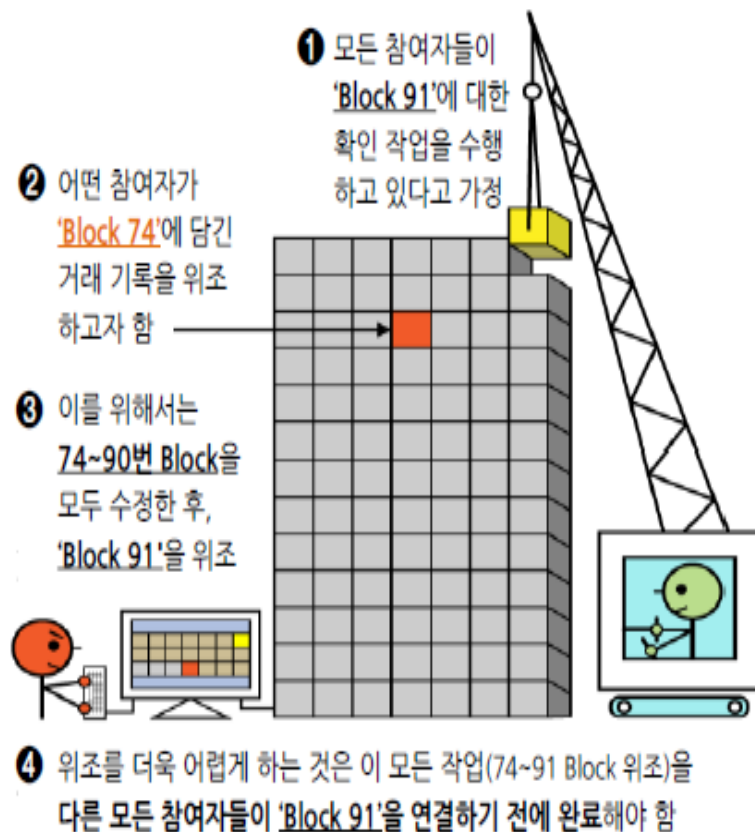
작동 원리

[그림3] 블록체인의 작동 프로세스



자료: FT(2015. 11. 1)

[그림4] 블록체인 위조가 어려운 이유



자료: IEEE Spectrum(2015. 7)

블록체인 특성

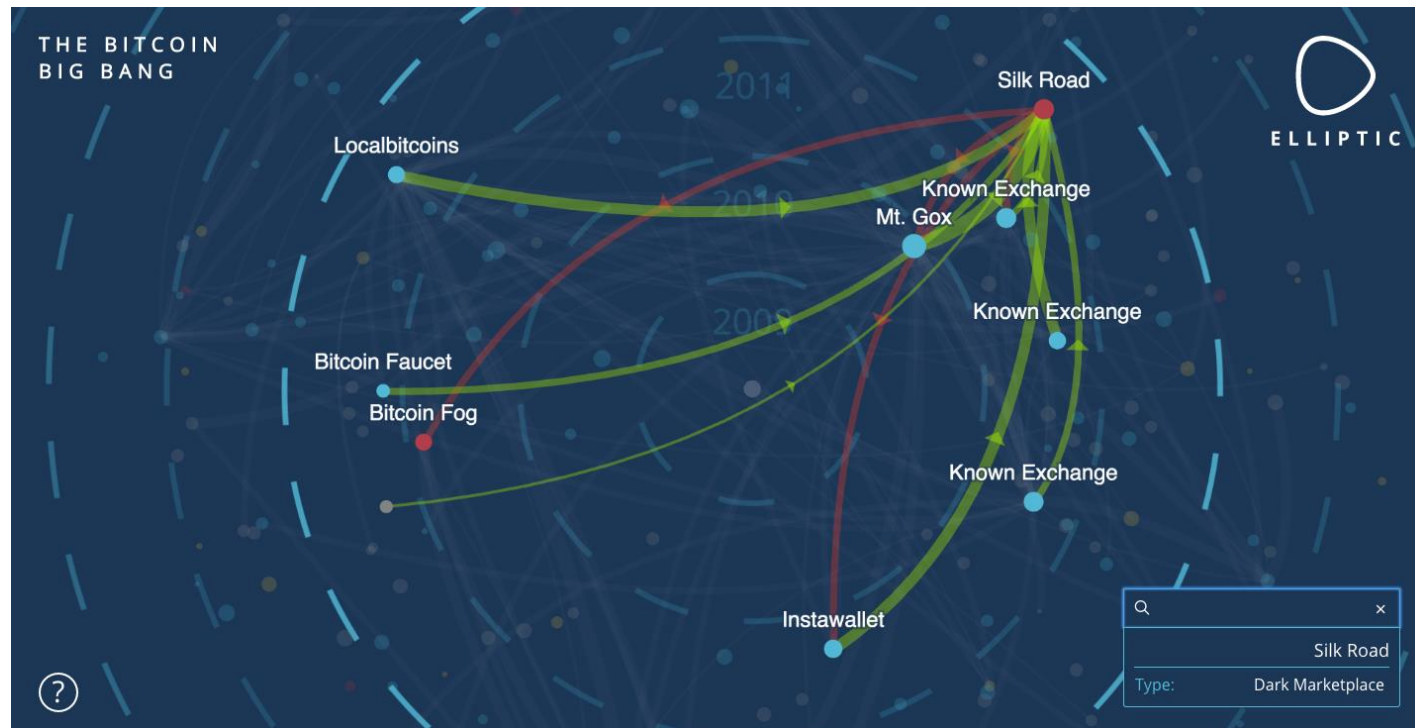
- 비트코인을 위해 고안된 원장 저장 시스템
- 블록에 거래기록 저장
- 모든 노드가 모든 복제된 블록(원장) 저장되고 체인(Chain)으로 연결되어 **불가역적(Immutable)하도록 설계됨**
- 거래자는 퍼블릭키에 의해 인식됨
 - 기본적으로 가명성(Pseudonymity) 제공
- 네트워크환경에서 구동되는 **시스템에 신뢰성 제공가능**
- 중앙의 권위 혹은 제3자(TTA)의 보증에 의존하지 않고 **사용자와 사용자간(Peer to Peer, P2P) 직접 가치전송**

블록체인 장점

- 투명성(Transparency)
- 자기부인방지(Non-repudiation)
- 확장성(Scalability)
- 보안성(Security)
- 탈중앙성(Decentralized)



신뢰성!



경제 (금융)

- “중앙은행 발행 디지털화폐의 거시경제”
 - 미국경제 가정 분석
 - 중앙 정부 채권에 대해 GDP의 30%를 디지털화폐를 발행하면 실질금리, 왜곡된 세금, 금융거래 비용 감소 등의 요인으로 GDP 3% 증가



BANK OF ENGLAND

Staff Working Paper No. 605

The macroeconomics of central bank issued digital currencies

John Barrdear⁽¹⁾ and Michael Kumhof⁽²⁾

Abstract

We study the macroeconomic consequences of issuing central bank digital currency (CBDC) — a universally accessible and interest-bearing central bank liability, implemented via distributed ledgers, that competes with bank deposits as medium of exchange. In a DSGE model calibrated to match the pre-crisis United States, we find that CBDC issuance of 30% of GDP, against government bonds, could permanently raise GDP by as much as 3%, due to reductions in real interest rates, distortionary taxes, and monetary transaction costs. Countercyclical CBDC price or quantity rules, as a second monetary policy instrument, could substantially improve the central bank's ability to stabilise the business cycle.

블록체인 기반 디지털 화폐

- 싱가포르
 - 이더리움 기반 화폐 연동
- 스웨덴은행
 - 2019년까지 블록체인기반 화폐 발행을 목표로 기술적 연구 진행 중
- 영란은행, 중국인민은행 등 검토 중
- 러시아 중앙은행 검토 중
- 캐나다 중앙은행 검토 후 포기

옌렌의장 중앙은행 연례회의에서 블록체인 연구 촉구



Yellen Reportedly Urges Central Banks to Study Blockchain, Bitcoin

By Graham Rapier
June 6, 2016



Federal Reserve Chairman Janet Yellen encouraged her fellow central bankers to accelerate their studies of new financial technologies, specifically mentioning bitcoin, the blockchain, and other distributed ledgers, according to the trade group whose conference she attended.

The June 1 event in Washington, attended by representatives from more than 90 central banks, was closed to the press. The Chamber of Digital Commerce, which organized the conference, summarized her

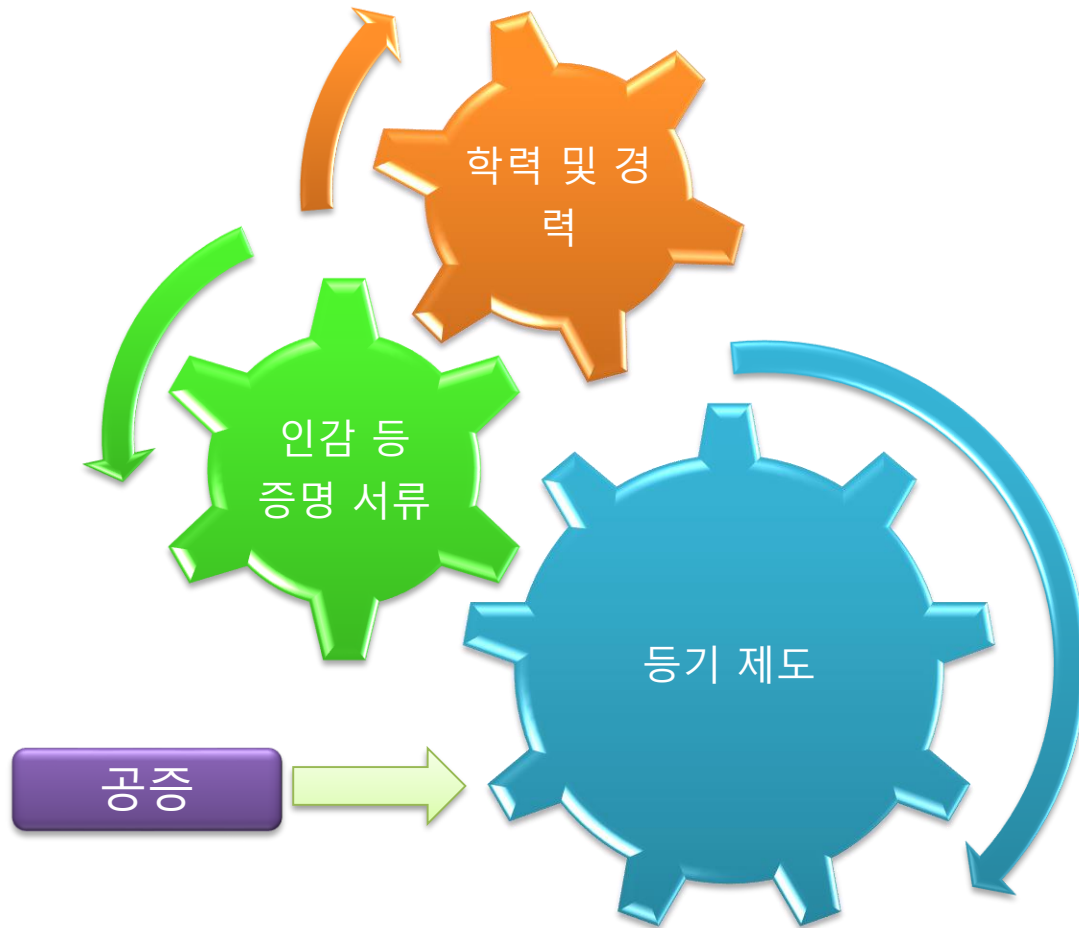


The Fed chair with Adam Ludwin, CEO of the tech startup Chain, and blockchain industry advocate Perianne Boring.

사회

오프라인 인증 대체수단으로서 블록체인

오프라인 인증제도



온라인 인증제도

공인인증서

신체 특징 인식

- 얼굴인식
- 지문인식
- 홍채인식
- 정맥인식

행동 인식

- 사인인식
- 자판입력인식
- 걸음걸이인식

Blockchain

블록체인 기반 국가 기록 관리

- 온두라스
 - 토지 등기부
- 투표관리
 - 에스토니아

정치

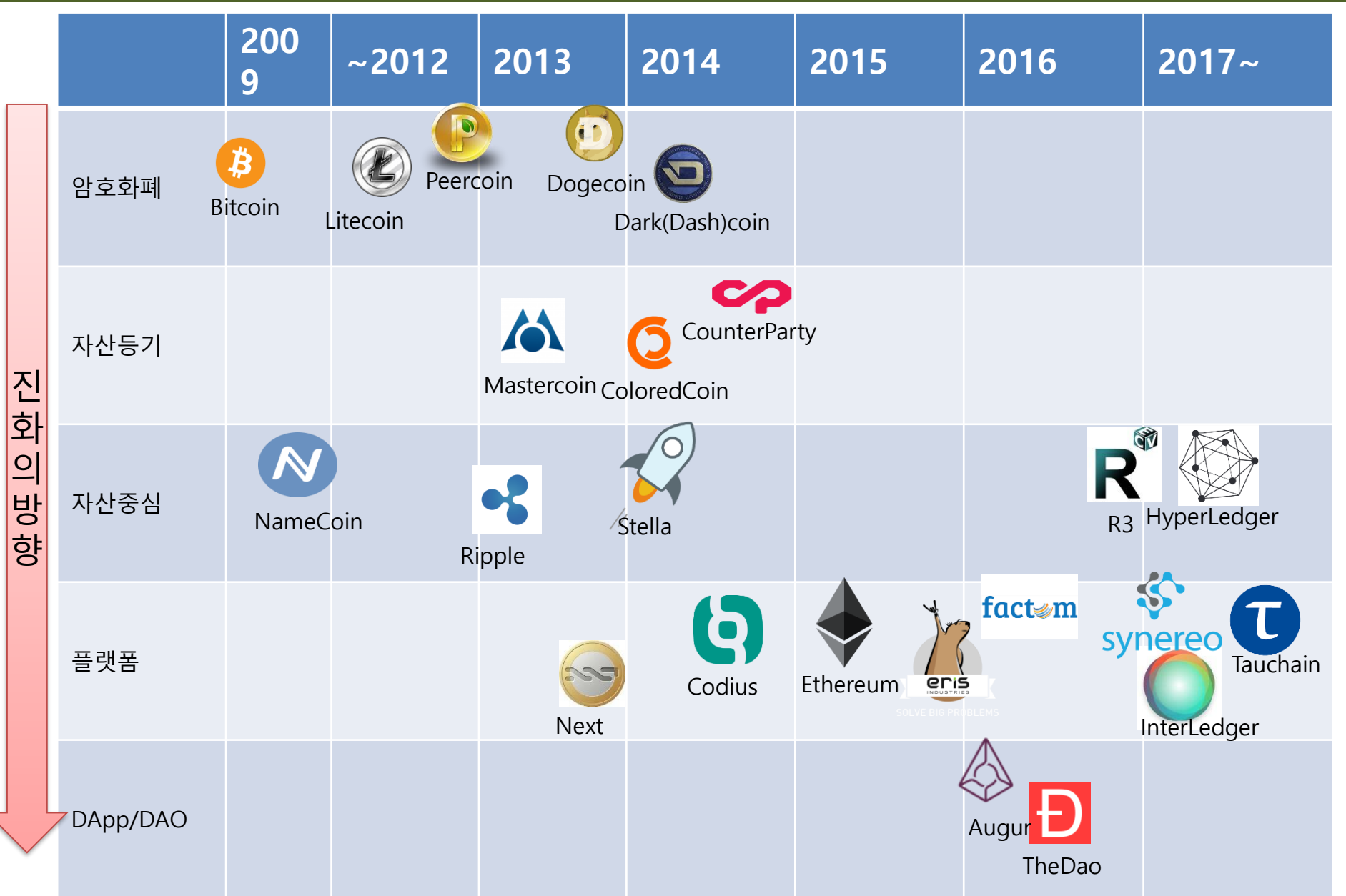
블록체인 기반 신생 정당

- 호주
 - 플렉스 당
- 스페인
 - 포데모스 당
- 덴마크
 - 자유연합(Liberal Alliance)
- BitNation
 - 국가 형태의 서비스 제공
 - 법적 결혼

문제는?

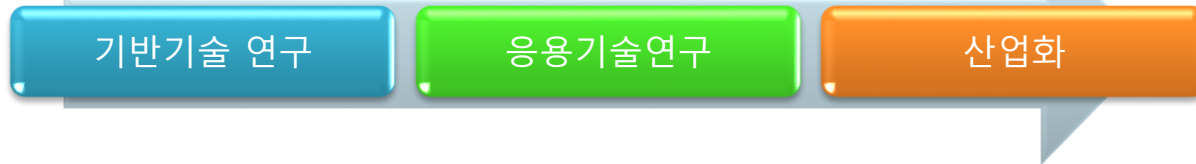
1. 학문적 연구부족
2. 자원낭비
3. 중국의존적 가격 형성
4. 성능
5. 해킹/범죄
6. 규제

블록체인기술 진화 방향



학문적 연구부족

일반적 기술 산업화 과정



비트코인의 경우



대부분의 ICO

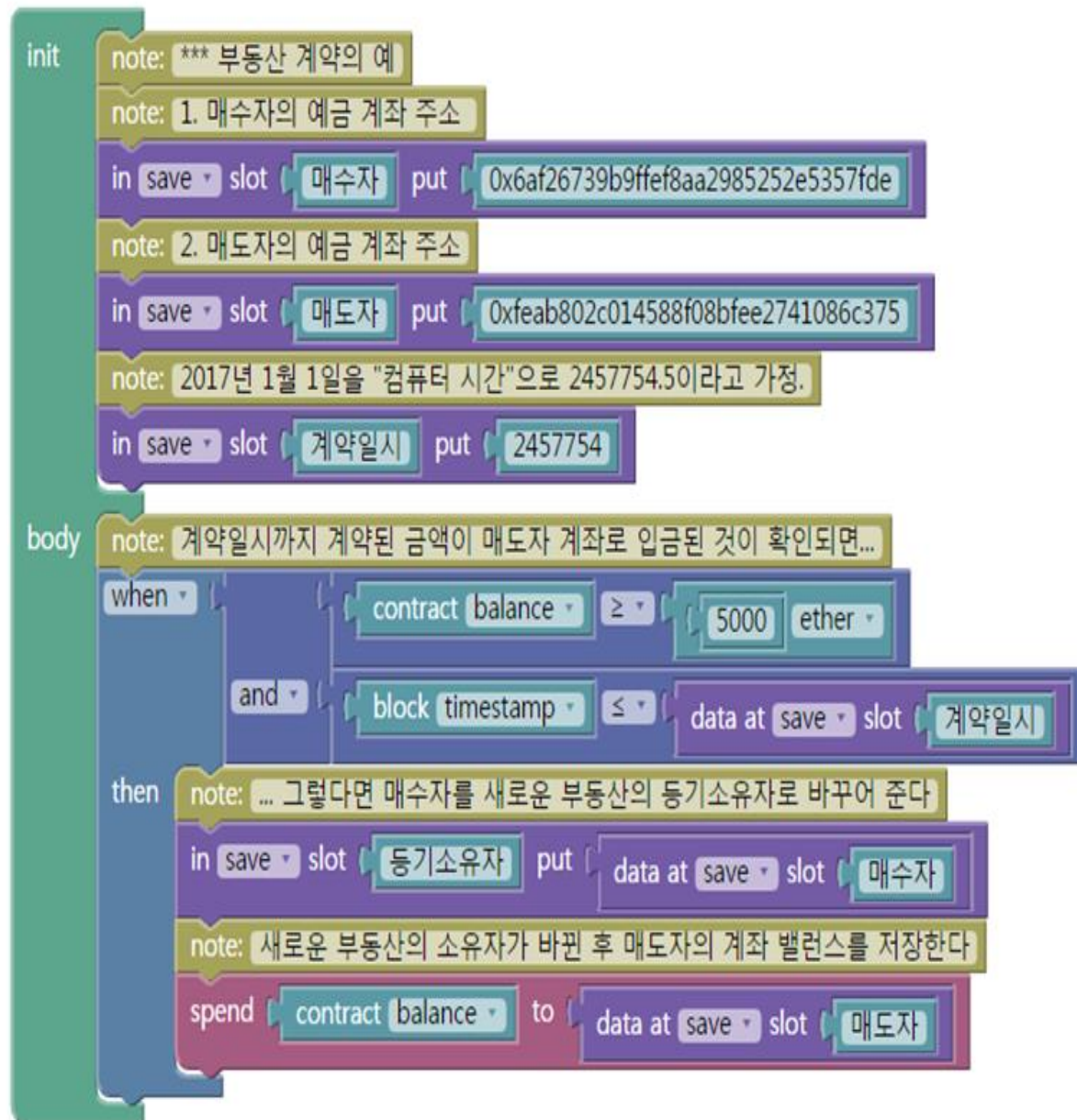


이더리움

이더리움은 스마트 계약을 위해 설계된 플랫폼

- 튜링완전성 제공
(튜링머신은 앨런 튜링이 만든 추상적 개념의 기계로 우리가 보통 쓰는 CPU를 가진 컴퓨터로 보면 됨. 튜링완전성은 튜링기계와 같은 수준의 성능을 갖는 성질을 말함. 이더리움이 튜링완전성을 갖는다는 말은 우리가 평소 사용하는 컴퓨터와 같은 정도의 강력한 성능을 갖는다는 의미의 단어임.)
- 분산자동단체(DAO; Decentralized Autonomous Organization)의 가능성 제공
- 이더리움은 그 강력한 성능에 의해 도전받는 중
 - 2016년 6월 TheDAO 해킹 사고 : 5천5백만불 도난
 - 2016년 9월 DoS (Denial of Service) 해킹 사고
 - 2017년 7월 CoinDash 해킹 사고 : 7백만불 도난

이더리움: 부동산 스마트계약의 예



자원낭비

초기 마이닝

Started as a hobby.



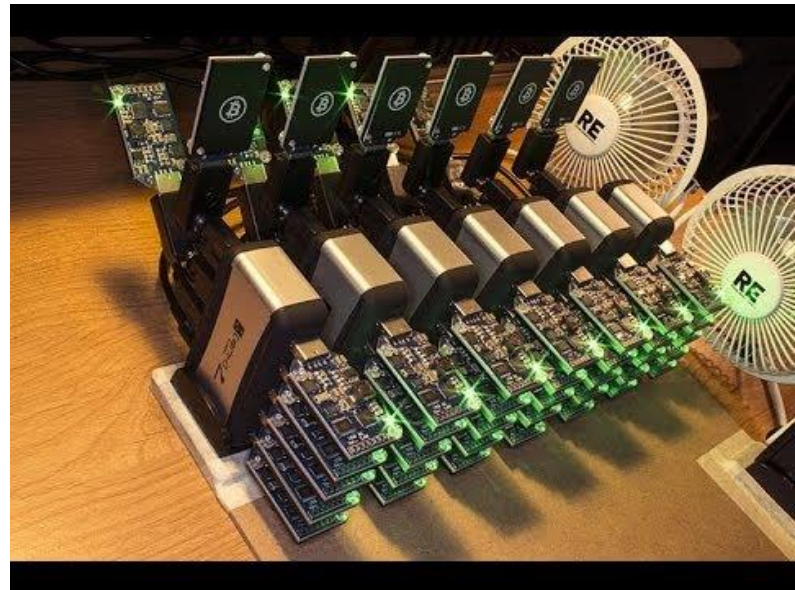
마이닝 기기 발달

Around 2011/2013

FPGA's
(field programmable gate array)



ASIC's
(application-specific integrated circuit)



마이닝 공장

Hobby has no chance.

An enormous bitcoin mine went up in flames, affecting the entire network

SHARE



WRITTEN BY

Kabir Chibber

OBSESSION

Digital Money

November 08, 2014



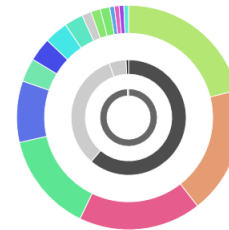
(Flickr/Coindesk)

A large bitcoin mining facility in Thailand [went up in flames](#) this week, destroying the five-megawatt operation and disrupting the cryptocurrency's entire network.



Pool Distribution %

24h 1W 1M 6M 1Y Max



Pool	Blocks	%
DiscusFish / F2Pool	31	21.09%
AntPool	27	18.37%
Bitfury	26	17.69%
BTCC	21	14.29%
Slush	13	8.84%
KNCMiner	5	3.40%
Telco 214	5	3.40%
21 Inc.	5	3.40%
BW Pool	4	2.72%

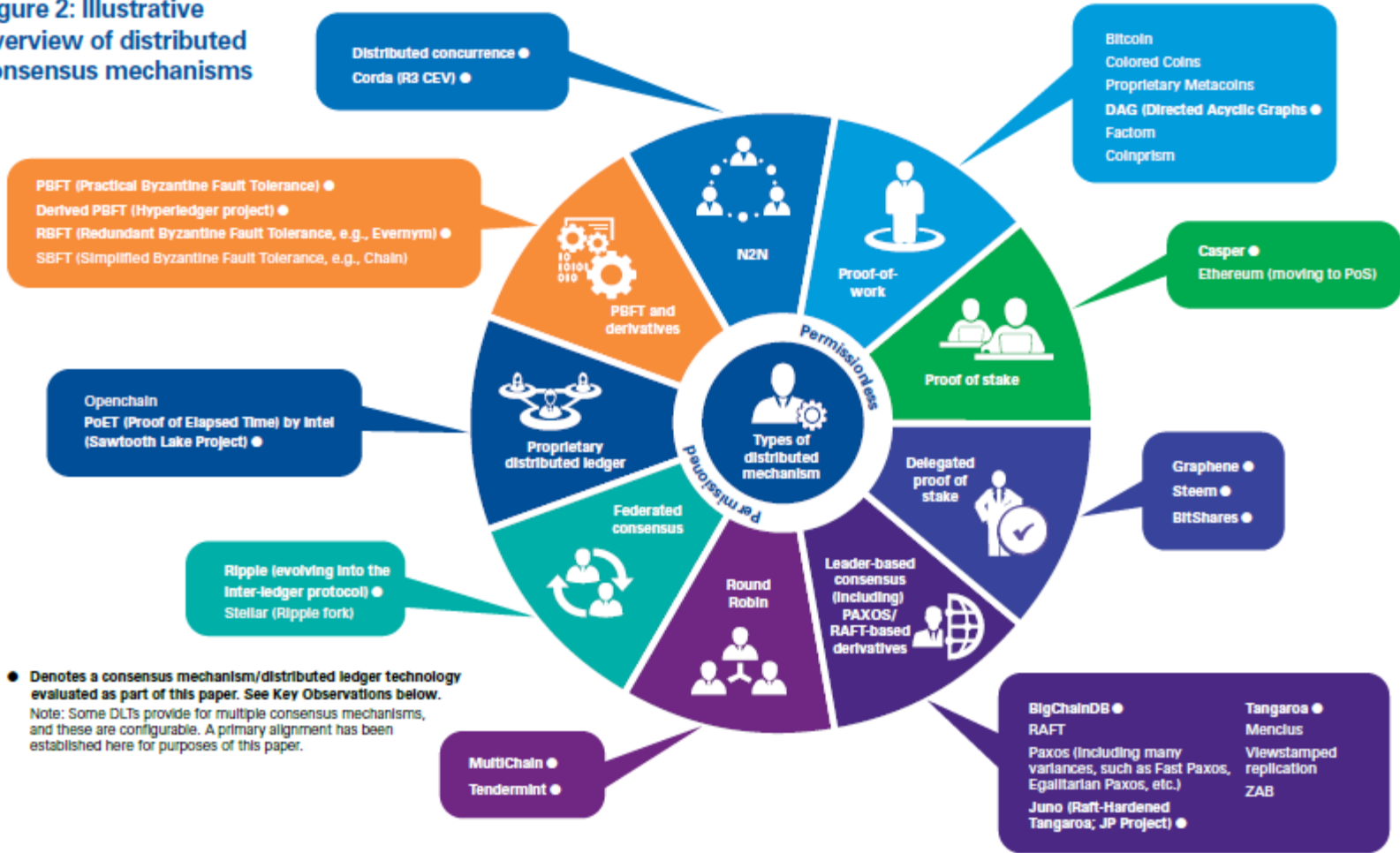
(src)

마이닝 공장



자원낭비 대안: 다수의 컨센서스 방법 사용 중 (혹은 제안 중)

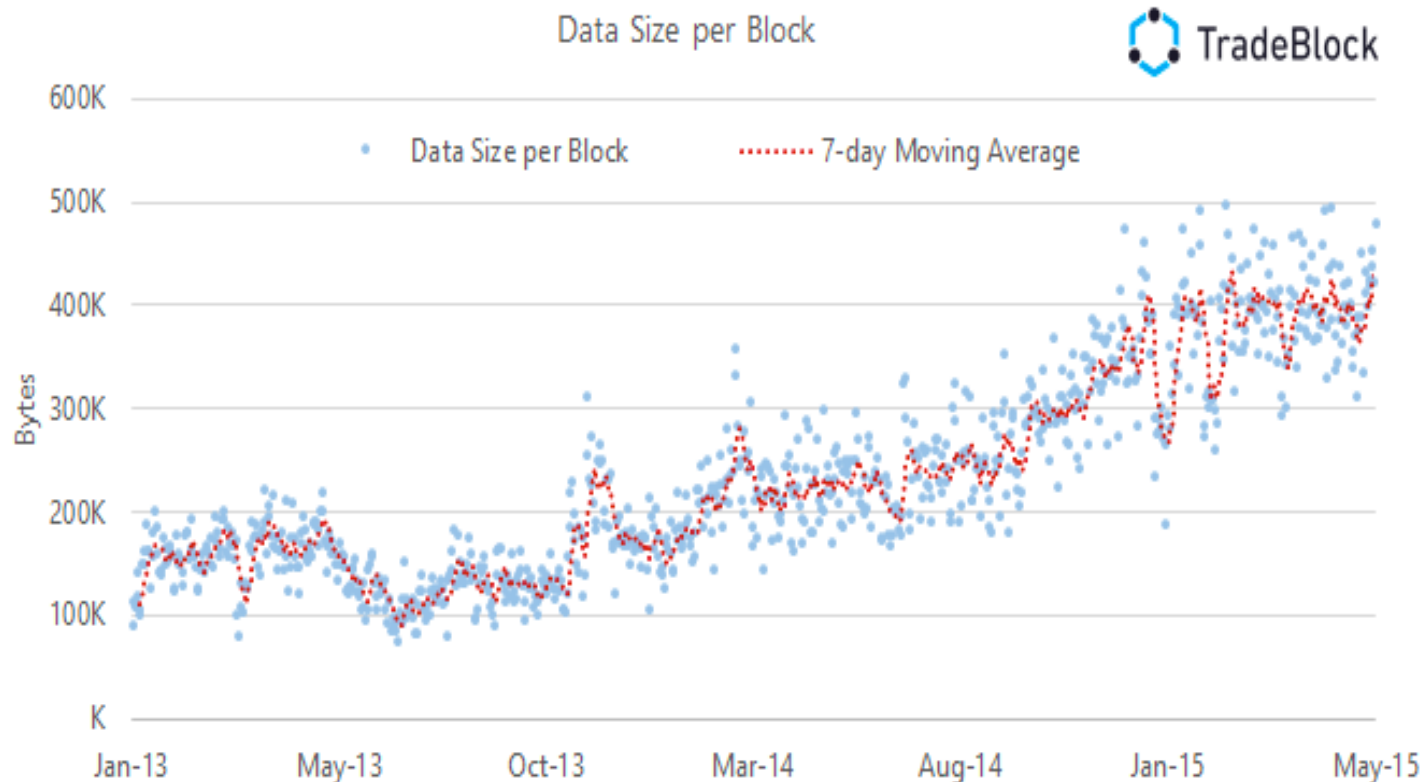
Figure 2: Illustrative overview of distributed consensus mechanisms



성능

저장 데이터 + 블록형성 속도

- **Total size of all blocks: ~95 Gbytes, 1MB/Block**
- A block in about a 10-minute time-span, ~7 transactions/min.

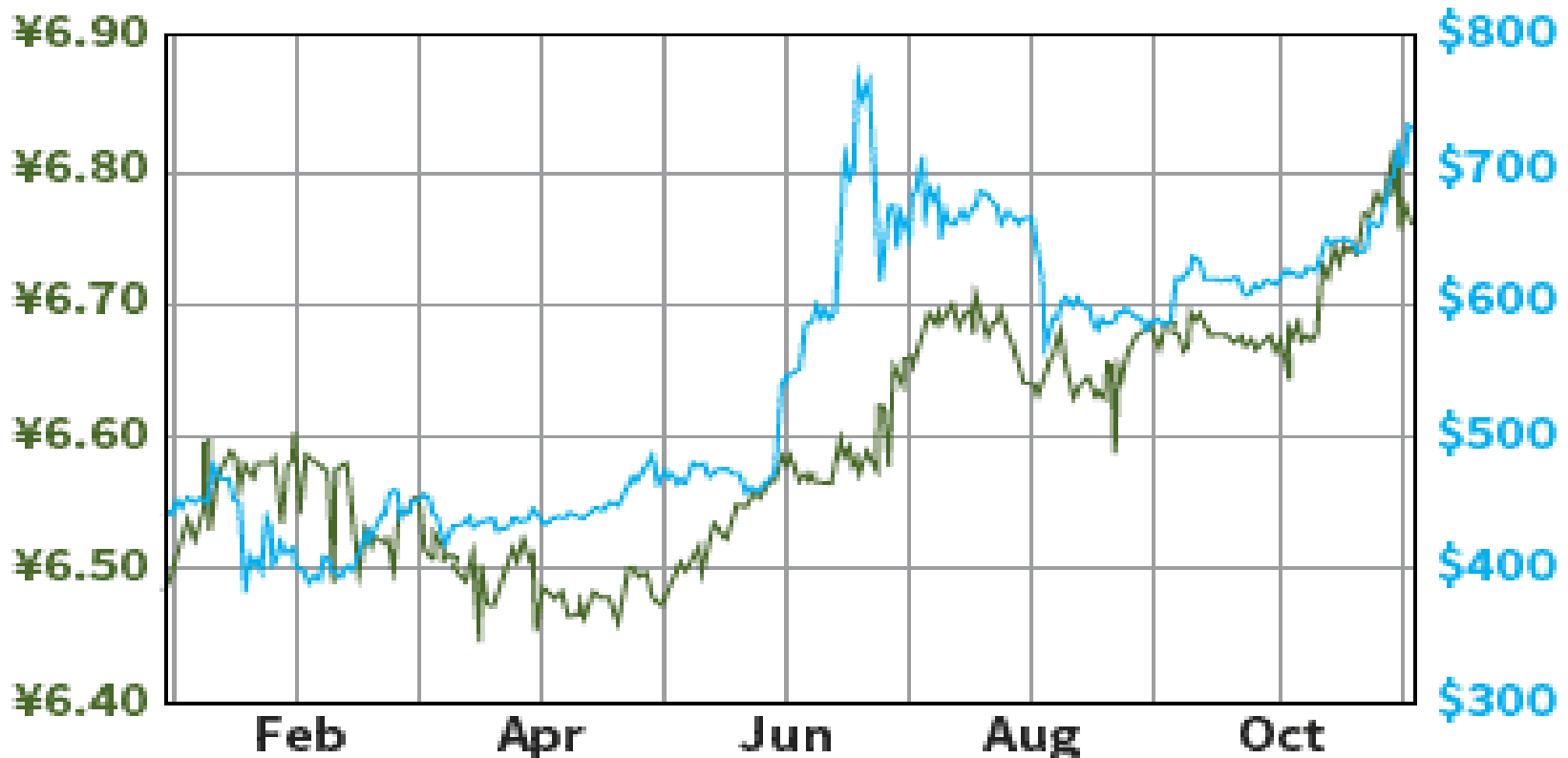


중국의존적 가격 형성

중국 정부의 정책에 의해 시장 가격 결정

Weaker Yuan Helps Push Bitcoin Higher

The weakening of the Chinese yuan this year has roughly matched Bitcoin's gains, particularly over the last month. This chart is inverted (showing the rising amount of yuan per dollar) to make the relationship more clear.



Sources: CoinDesk, XE.com, Money Morning Staff Research

해킹과 범죄의 대상

범죄

- 실크로드: 마약, 불법 총기류 등 거래

Welcome! | Silk Road - Tor Browser

File Edit View History Bookmarks Tools Help

Welcome! | Silk Road Full Tutorial - Installing Tails Live...

silkroadvb5piz3r.onion

Silk Road
anonymous market

messages 0 | orders 0 | account B0.0000

Search Go

Shop by Category

- Drugs 12,027
 - Cannabis 2,784
 - Dissociatives 201
 - Ecstasy 1,253
 - Intoxicants 63
 - Opioids 361
 - Other 36
 - Precursors 87
 - Prescription 3,710
 - Psychedelics 1,253
 - Stimulants 1,462
 - Tobacco 316
- Apparel 536
- Art 13
- Biotic materials 2
- Books 1,158
- Collectibles 20
- Computer equipment 106
- Custom Orders 86
- Digital goods 854
- Drug paraphernalia 441
- Electronics 168
- Erotica 739
- Fireworks 9
- Food 13
- Forgeries 136
- Hardware 49

GRAND OPENING SALE!
PURE UNCUT COCA
B6.4234

TWEETB
TOP SHELF MEDICAL GRADE
MANGO
+MANGO+ 1g
B0.2467

1 OZ P. Cubensis Shroom
Capsules
B1.5831

0.5g Hi-Heat Cocaine - Scott
& Purity Tested
B0.7262

10pcs Green Android
220mg PURE MDMA xtc pills
B1.0166

+SFV OG KUSH+ 1g
B0.2467

Free Ross-A-Thon Dedicated To Raise Awareness Of The Silk Road Case

The controversial arrest and sentencing of the Silk Road founder Ross Ulbricht remain a thorn in many people's sides, including his mother, Lyn Ulbricht.

Ross was sentenced to life in prison without parole last May 2015 for non-violent charges and has been fighting for his freedom ever since.

ANNOUNCEMENT: Silk Road 3.0 is BACK ONLINE and open for business. The team did a massive security overhaul on the site to try and make it more secure and anonymous.

[>> Click here to find the Silk Road 3.0 Guide <<](#)

His latest breakthrough came in the form of an appeal to an appellate bench of judges in Manhattan earlier, and now a number of high profile individuals in technology and human rights are getting behind his efforts to see what liberty

Event Aims to Raise Awareness and Funds

The Free Ross-A-Thon event will be held on December 4 and will focus on raising funds and awareness concerning the Silk Road case in efforts to get the world to see what liberty author Doug Casey has called "a gigantic injustice."

The Free Ross-A-Thon event will be hosted by **Ulbricht's mother, Lyn Ulbricht**, alongside Terry Brock and Tatiana Moroz.

It will also feature some prominent appearances from high-profile individuals including Deep Web director Alex Winter, radio show host Tom



Free Ross-A-Thon Event Aims to Promote Freedom

범죄

- **마운트 곱스 거래소:** 당시 최대 비트코인 거래소. 약 4억5천만달러에 달하는 양의 비트코인을 해킹 당했다고 주장. 조사결과 거래소의 대표가 도둑질한 것으로 판명되었으나 증거부족으로 대부분의 혐의에 대해서 무죄 판결.

Mark Karpeles Posts Bail and Weighs a Lot Less

Mark Karpeles was arrested last year by Japanese authorities for being involved with the Mt Gox fiasco, losing roughly 700 thousand Bitcoins. Prosecutors are accusing Karpeles of embezzling \$3.4 million after his company filed for bankruptcy. Karpeles has been arrested two times so far for moving money.

トップ > 社会 > ビットコイン巨額消失 カルプレス被告保釈



ビットコイン巨額消失 カルプレス被告保釈

ツイートする

シェアする

2016年7月14日 20:35



해킹

- 2009년부터 2015년까지 비트코인 거래소의 3분의 1이 해킹당하고 그 중 반은 그 결과로 폐쇄됨.

Bitfinex: Cause of Bitcoin Hack Still 'Unknown'

Stan Higgins (@mpmcsweney) | Published on August 17, 2016 at 15:18 GMT

NEWS



Nearly two weeks after losing more than \$60m in customer funds, Bitfinex reports it has not yet identified how the theft was carried out.

In a [statement](#) released earlier today, the exchange reported it had hired Ledger Labs, a blockchain consultancy previously contracted by ShapeShift following [its own cybersecurity problems](#), to both investigate the theft as well as perform a balance sheet audit.



해킹 역사

시기	서비스명	서비스 종류	피해금액
2011. 6월	Mt.Gox	거래소	875만달러
2011. 8월	MyBitcoin	거래소	80만달러
2012. 9월	Bitfloor	거래소	25만달러
2013. 4월	Instawallet	지갑서비스	460만달러
2013.10월	Inputs.io	지갑서비스	100만달러
2013.10월	Global Bond Limited	거래소	500만달러
2014. 2월	Mt.Gox	거래소	4억5천만달러
2014. 3월	Flexcoin	은행(비트코인 보관)	65만달러
2014. 3월	Polenix	거래소	5만달러
2014. 8월	BTER	거래소	165만달러
2015.10월	Blockchain.info/ LocalBitcoins사용자	개인	25만불(추정)
2015.11월		개인	
2015. 1월	Bitstamp	거래소	500만달러
2015. 2월	BTER	거래소	175만달러
2015. 2월	Cavirtex	거래소	0달러, 거래소 폐쇄
2015. 3월	Coinapult	거래소	4만3천달러
2015. 5월	Bitfinex	거래소	43만달러
2015. 6월	Scrypt.CC	클라우드 마이닝	미상
2015. 10월	Purse.io	비트코인(아마존연결 쇼핑)	30만달러
2016. 6월	The Dao	크라우드 펀딩	5천5백만달러
2016. 8월	Bitfinex	거래소	7천만달러

원 자료: 한국은행(2015년이후 자료 추가)

폰지 사기



Charles Ponzi

Buyer Beware! The Definitive OneCoin Ponzi Exposé

By *Jamie Redman* - June 27, 2016 299074 1018

SHARE



암호화폐는 쉬운 사기 대상



- 오로라코인
 - 2014년 1월 24일 론칭
 - 공중살포: 모든 아이슬란드 국민은 31.8 오로라코인(AUC)
 - 2014년 3월 25일
 - 국민: ~33만 → 10.5M
 - 2014년 5월 이후 쓰레기가 됨.
 - Founder 50% 소유. (10.5M of 21M)
 - 시중에 3.4M 풀림
 - 비트코인 소유
 - 신뢰성?

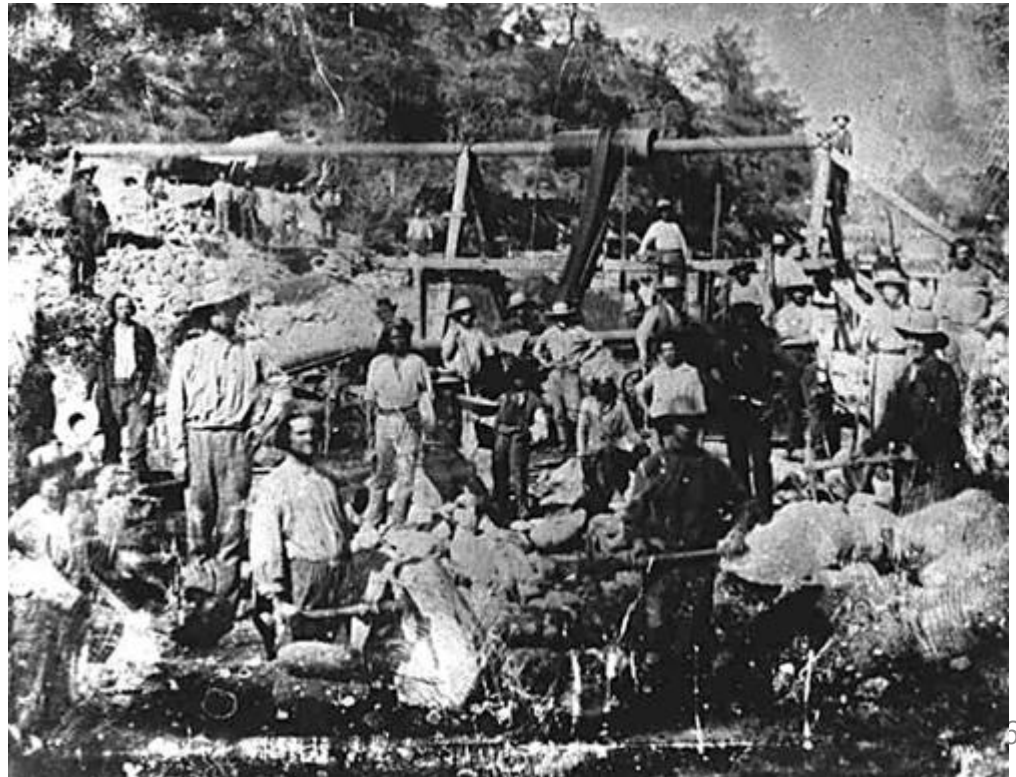
- +

▲ 웨호스팅 업체 인터넷나야나의 홈페이지 공지문

무규제 영역

무규제 - 약육강식 무법지대

- 미국 캘리포니아 골드러쉬와 유사
 - 약 30만명 인구 캘리포니아 이주
 - 캘리포니아 거주 (인디안) 원주민 대학살 단초
 - 기술 발전과 인프라형성을 통한 경제 활성화
- ICO 대부분 비정상적 형태 사업



규제준수 어려움

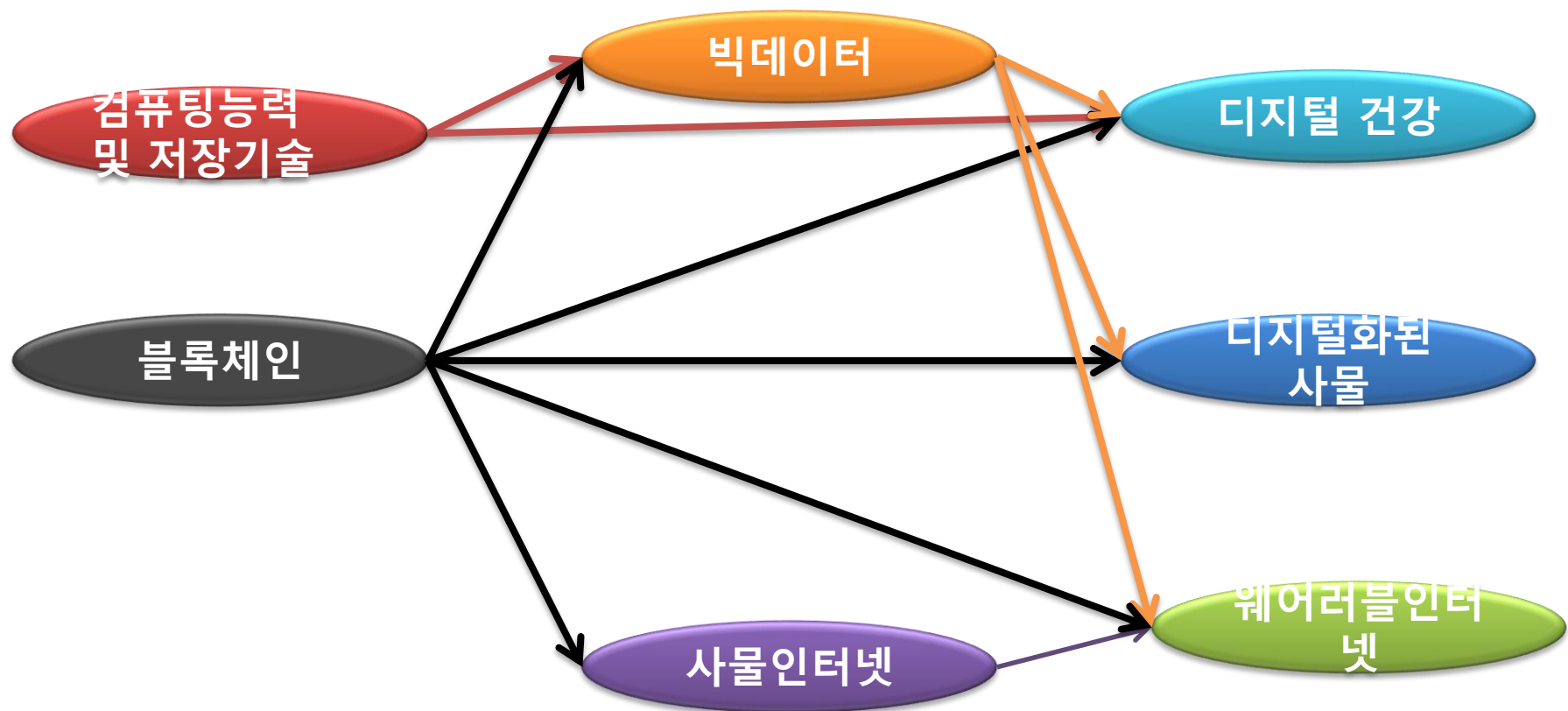
- 금융규제법
 - AML(자금세탁방지법)
 - 막대한 자금이 세탁되고 있는 중
 - KYC(고객파악규정)
- 개인정보보호법
- 잊혀질 권리 (Right to be forgotten) 처리

결론

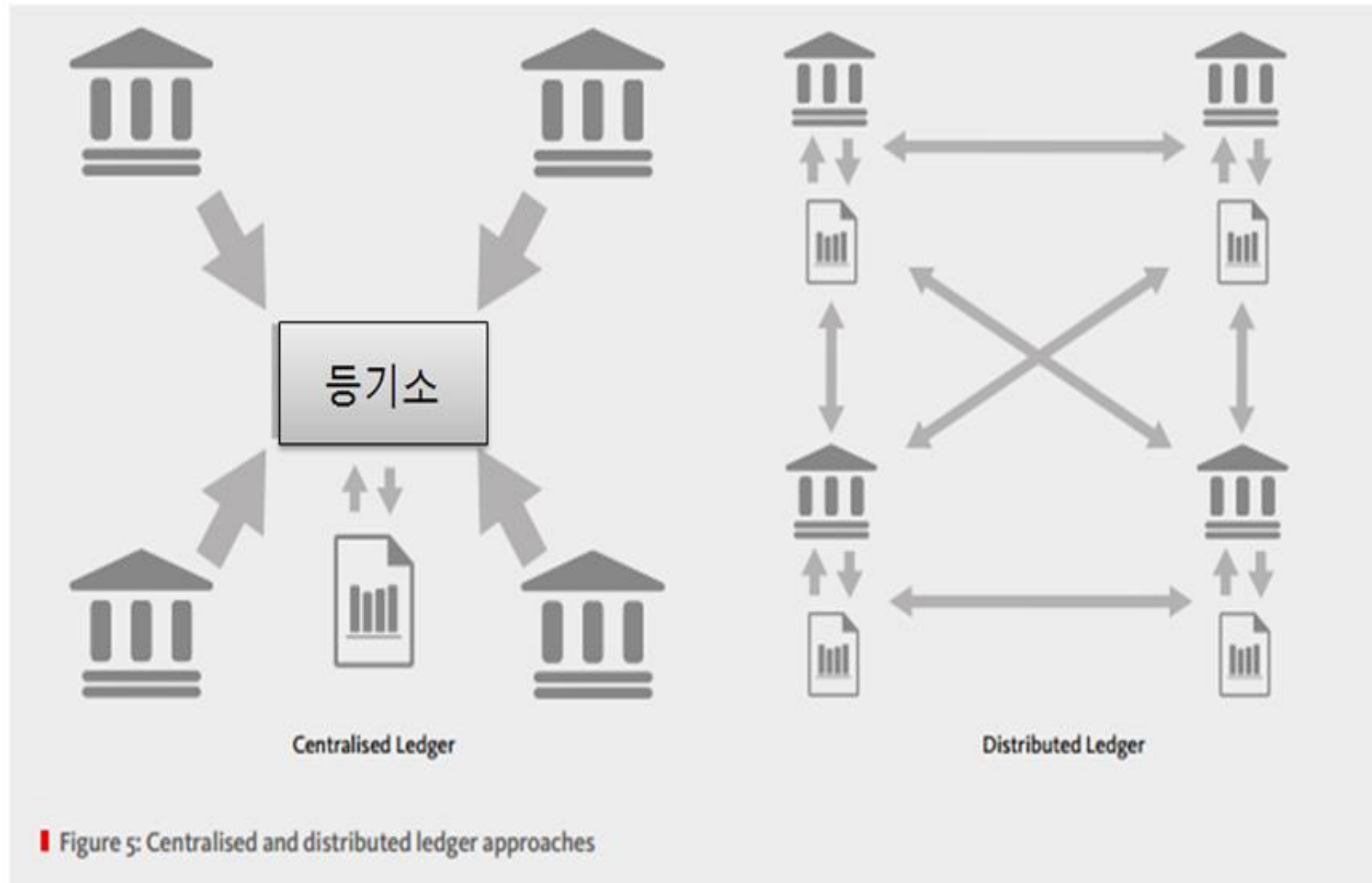
- 블록체인에 대한 미래 예측
- 국가전략
- 가장 시급한 당면 문제?

블록체인에 대한 미래 예측

인프라 기술로서 분산원장



이더리움: 종래의 등기시스템과 스마트계약 비교





국가전략

국제적 블록체인 기술 주도권: 표준화

실질적 표준

- **W3C**
 - 블록체인 온톨로지
 - 유스케이스

제도적 표준

- **ISO**
 - 참조구조
 - 보안, 정보보호
 - **아이덴티티**
 - 스마트계약
 - 유스케이스

국가디지털ID관리시스템 (National Digital Identity Management System)

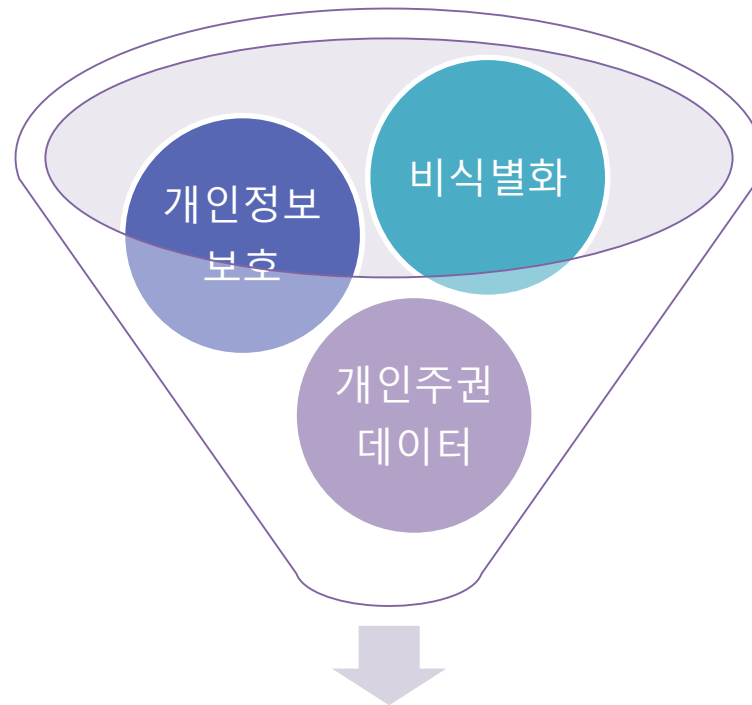
PKI 방식

한국, 네덜란드, UK, 에스토니아, 인디아, 미국(?)

블록체인기반 방식

ISO에서 표준화 중

각종 국가기록 활용을 위한 블록체인



블록체인 기반 빅데이터활용

사회적 신뢰 제공 시스템으로서 블록체인



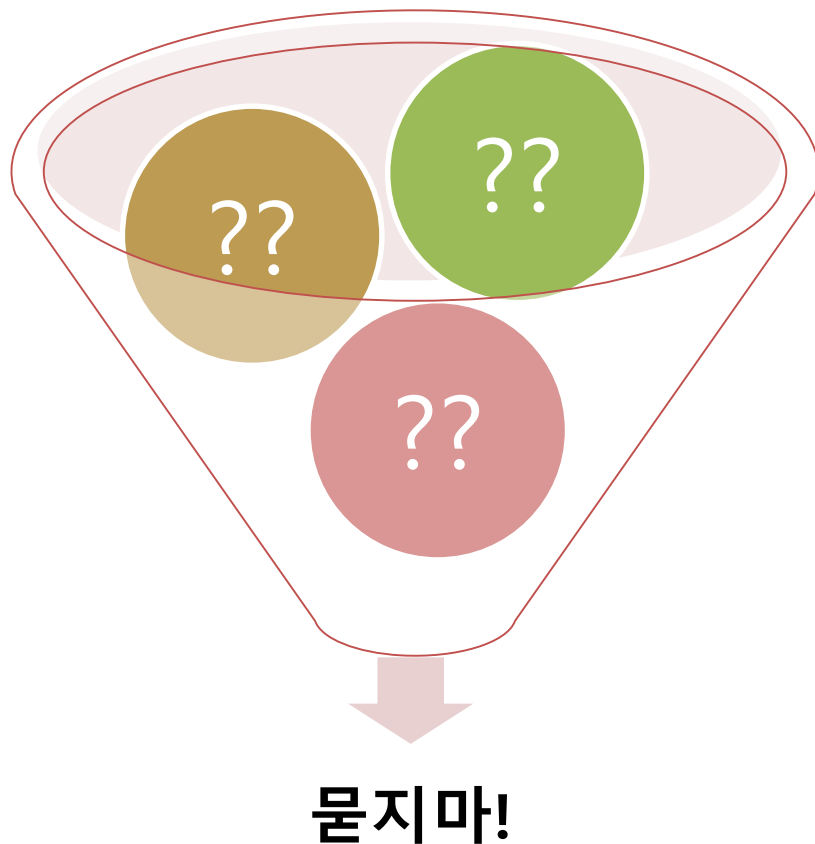
가장 시급한 당면 문제?

[Charts](#) [Markets](#) [Social](#) [Tools](#)

Ethereum Markets

#	Source	Pair	Volume (24h)	Price	Volume (%)
1	Bithumb	ETH/KRW	\$249,071,000	\$382.76	15.14%
2	Coinone	ETH/KRW	\$199,455,000	\$383.07	12.13%
3	GDAX	ETH/USD	\$169,567,000	\$351.57	10.31%
4	Poloniex	ETH/BTC	\$126,768,000	\$361.64	7.71%
5	OKCoin.cn	ETH/CNY	\$93,436,400	\$377.98	5.68%
6	Kraken	ETH/EUR	\$87,767,800	\$355.46	5.34%
7	Korbit	ETH/KRW	\$82,451,500	\$383.03	5.01%
8	Huobi	ETH/CNY	\$78,065,200	\$374.34	4.75%
9	Bitfinex	ETH/USD	\$67,570,200	\$347.53	4.11%
10	Gemini	ETH/USD	\$48,246,100	\$350.53	2.93%

묻지마 투자에 대한 해결책?



크립토 화폐에 대한 올바른 교육을 통한 계몽 시급!

Q&A

