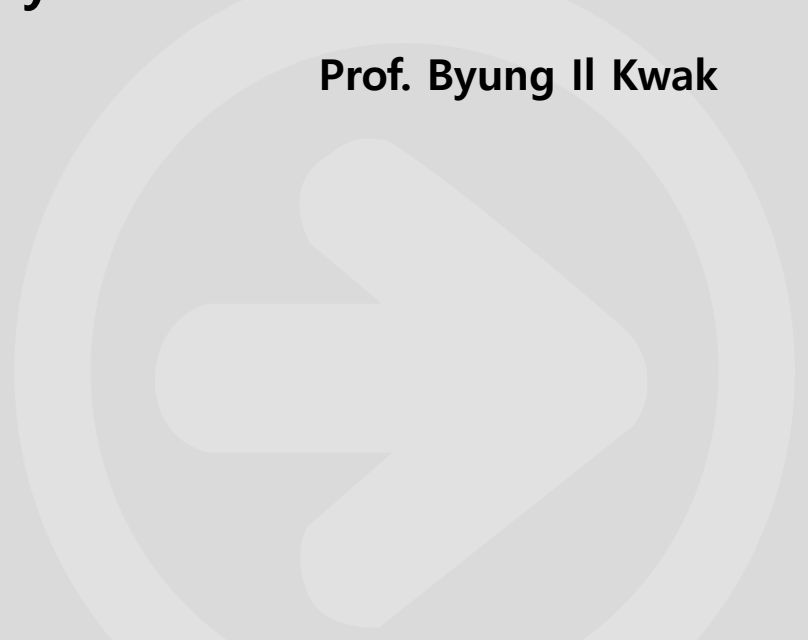




Blockchain #4

The history of bitcoin and blockchain

Prof. Byung Il Kwak



□ Cryptography

- ▣ 해시 함수와 전자 서명

□ 분산 네트워크에서의 시간 동기화

- ▣ 중앙화된 서버를 통한 시간 동기화
- ▣ 분산 네트워크에서의 해시 체인을 이용한 시간 동기화

□ Blockchain Details

- ▣ 블록체인 (트랜잭션 및 블록 생성)
- ▣ Public vs Private 블록체인
- ▣ 합의 (블록체인 Fork, 합의 모델)

CONTENTS

- ❑ The history of bitcoin

□ DigiCash

- ▣ 은닉 서명기능과 이중 지급을 방지하기 위한 비밀키 공유 기능을 가짐
 - 사용자가 자신의 신원을 공개하지 않고 거래를 승인하는 기능
- ▣ 중앙화 및 신용카드로 인한 대중화 실패

□ 해시 체인과 작업증명 (PoW)

- ▣ Satoshi Nakamoto: 익명의 비트코인 개발자가 백서를 작성
- ▣ Trustless blockchain 시스템을 개발함
 - 암호 해시 함수를 기반의 전자 결제 시스템

Bitcoin

Explorer >  Bitcoin Explorer > Block

 Search your transaction, an address or a block

USD ▾


Block 0 

USD **BTC**

This block was mined on January 04, 2009 at 3:15 AM GMT+9 by [Unknown](#). It currently has 697,509 confirmations on the Bitcoin blockchain.

The miner(s) of this block earned a total reward of 50.00000000 BTC (\$2,361,462.50). The reward consisted of a base reward of 50.00000000 BTC (\$2,361,462.50) with an additional 0.00000000 BTC (\$0.00) reward paid as fees of the 1 transactions which were included in the block. The Block rewards, also known as the Coinbase reward, were sent to this [address](#).

A total of 0.00000000 BTC (\$0.00) were sent in the block with the average transaction being 0.00000000 BTC (\$0.00). Learn more about [how blocks work](#).

Hash	00000000019d6689c085ae165831e934ff763ae46a2a6c172b3f1b60a8ce26f 
Confirmations	697,509
Timestamp	2009-01-04 03:15
Height	0
Miner	Unknown
Number of Transactions	1
Difficulty	1.00
Merkle root	4a5e1e4baab89f3a32518a88c31bc87f618f76673e2cc77ab2127b7afdeda33b
Version	0x1
Bits	486,604,799
Weight	1,140 WU
Size	285 bytes
Nonce	2,083,236,893
Transaction Volume	0.00000000 BTC
Block Reward	50.00000000 BTC




The history of bitcoin


□ Bitcoin


▣ 세대에서 가장 비싼 피자


– Bitcoin의 첫번째 거래

 Author

Topic: Pizza for bitcoins? (Read 774776 times)

laszlo
Full Member


Activity: 199
Merit: 149


Pizza for bitcoins?
 May 18, 2010, 12:35:20 AM
Merited by alani123 (12), OgNasty (10), d5000 (5), EFS (1), vapourminer (1), iluvbitcoins (1), jacktheking (1), LoyceV (1), coolcoinz (1), Kda2018 (1), TheQuin (1), Toxic2040 (1), Toughit (1), nullius (1), alia_armelle (1) #1

I'll pay 10,000 bitcoins for a couple of pizzas.. like maybe 2 large ones so I have some left over for the next day. I like having left over pizza to nibble on later. You can make the pizza yourself and bring it to my house or order it for me from a delivery place, but what I'm aiming for is getting food delivered in exchange for bitcoins where I don't have to order or prepare it myself, kind of like ordering a 'breakfast platter' at a hotel or something, they just bring you something to eat and you're happy!

I like things like onions, peppers, sausage, mushrooms, tomatoes, pepperoni, etc.. just standard stuff no weird fish topping or anything like that. I also like regular cheese pizzas which may be cheaper to prepare or otherwise acquire.

If you're interested please let me know and we can work out a deal.

Thanks,
Laszlo

BC: 157fRrqAKrDyGHR1Bx3yDxeMv8Rh45aUet





The history of bitcoin

□ Bitcoin

- ▣ May 22, 2010, Laszlo Hanyecz \$25 가격의 피자 2판 구매하는데 10,000BTC를 지불
 - 현재가치: $10,000 \text{ BTC} \times 55,105,496 \text{ 원} = \text{대략 } 5510 \text{ 억}$
- ▣ Bitcoin이 과거와 달리 인터넷 상에서의 가치 없는 화폐에서 실제 가치가 있는 것으로 변화함



The history of bitcoin

□ Bitcoin 사건 사고

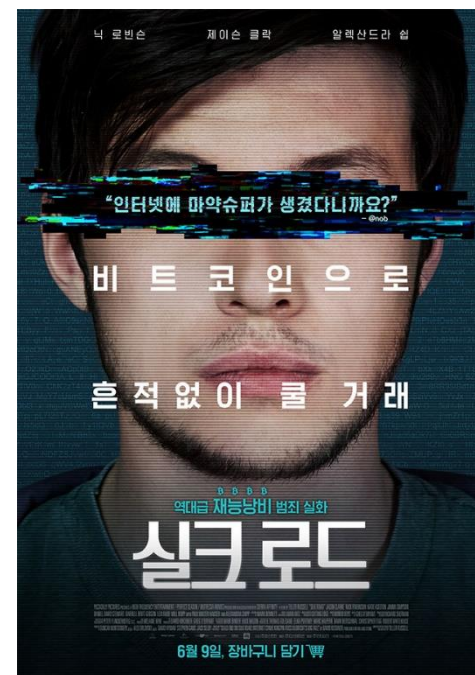
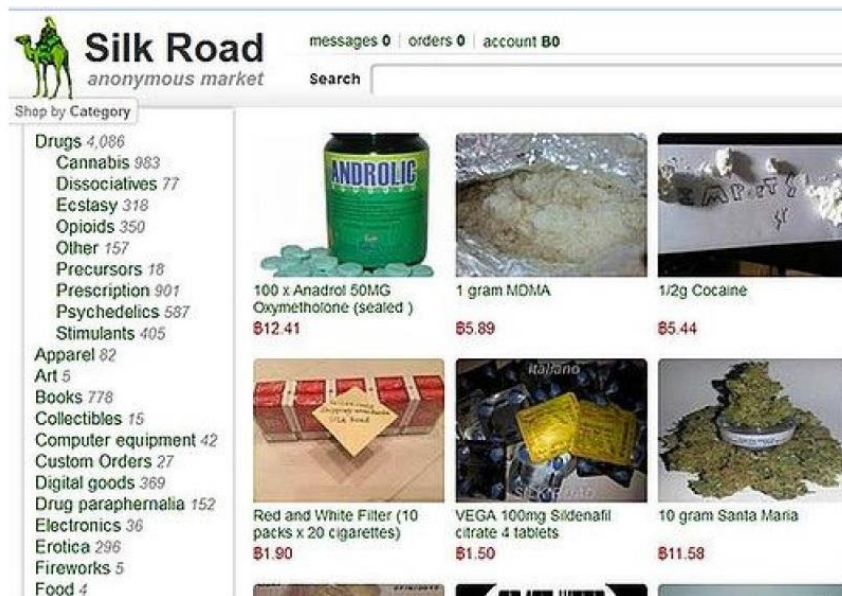
- 2010.08.15: Bitcoin 시스템 불안정성으로 인한 1840억 Bitcoin 생성
 - 프로토콜 업데이트로 수정됨
- 2013.10.29: 로보코인 (Robocoin) 과 비타코닉스 (Bitconiacs) 회사에서 Bitcoin 자동입출금기 (ATM) 설치
- 2014.2: Bitcoin 거래소 마운틴 곱스 (Mt.Gox)가 744,000 개의 Bitcoin 분실후 파산
- 2016.8: 비트피넥스 (Bitfinex) 거래소가 120,000개의 Bitcoin 분실
- 2021.4: Bitcoin가격이 8000만원 이상 돌파



The history of bitcoin

Bitcoin 사건 사고

- 2011.2: Tor와 Bitcoin을 사용하여 익명의 'eBay of Drugs'로 SilkRoad가 열림
 - 마약 및 암시장 상품이 Bitcoin의 사용 사례로 나타남
- 2013.10: FBI가 SilkRoad를 폐쇄하고 350만달러의 Bitcoin을 압수함





The history of bitcoin

□ Ransomware

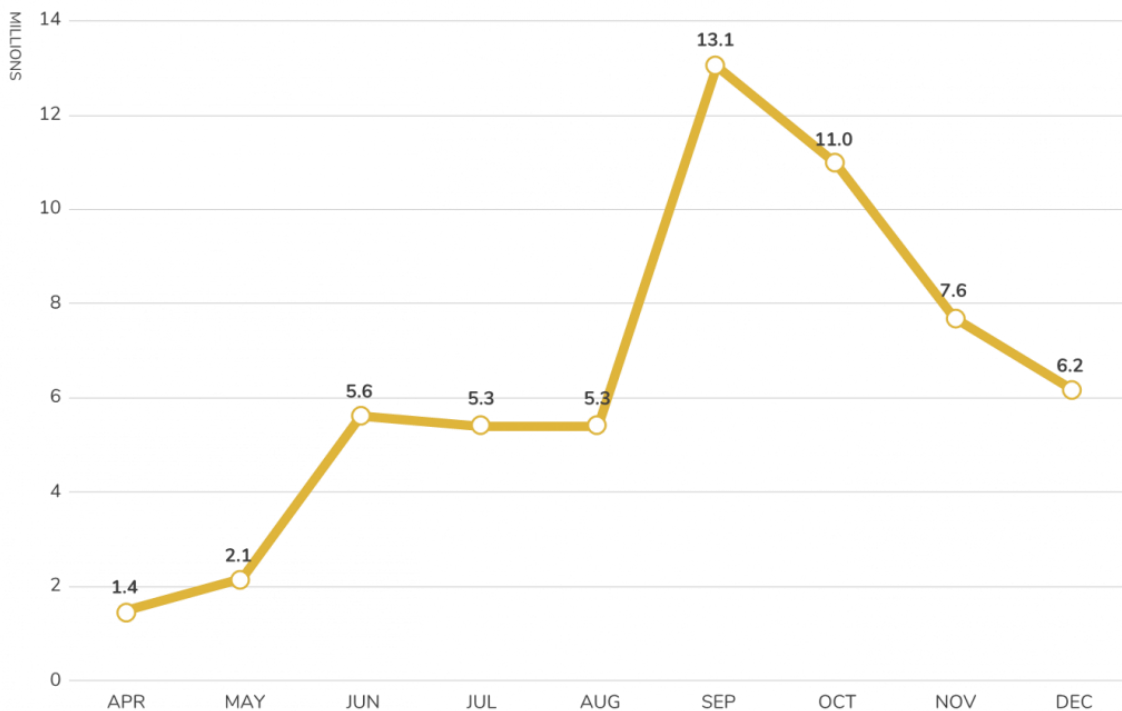
- ▣ Ransomware에 대한 암호를 풀기 위해 Bitcoin이 사용됨



The history of bitcoin

□ Cryptojacker

- ▣ 사용자의 PC를 Malware에 감염시켜 채굴 봇으로 변환 시킴

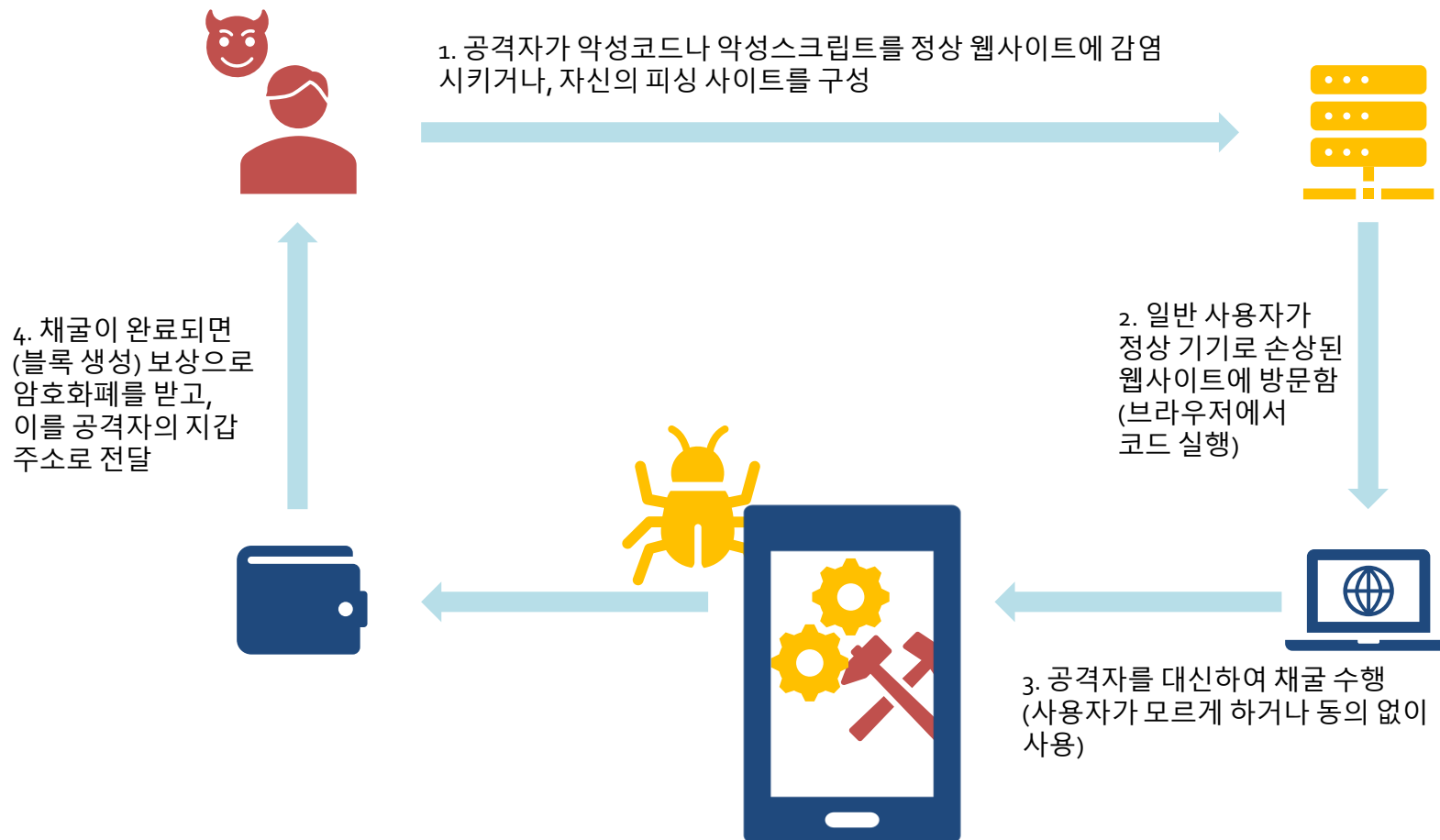


2018년도 Cryptojacker 공격 빈도



The history of bitcoin

❑ Cryptojacker - Browser-Based Cryptojacking



[Source: <https://sectigostore.com/blog/what-is-cryptojacking-how-to-define-explain-prevent-it/>]



The history of bitcoin

Bitcoin bubble

Bitcoin to KRW Chart





The history of bitcoin

Bitcoin bubble

Ethereum to KRW Chart



The history of bitcoin

□ Altcoins



Litecoin



ZCash



Stellar



Peercoin



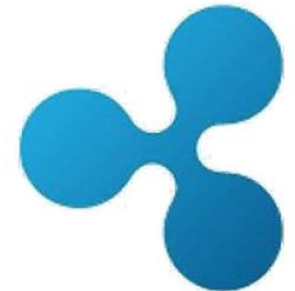
Dogecoin



DASH

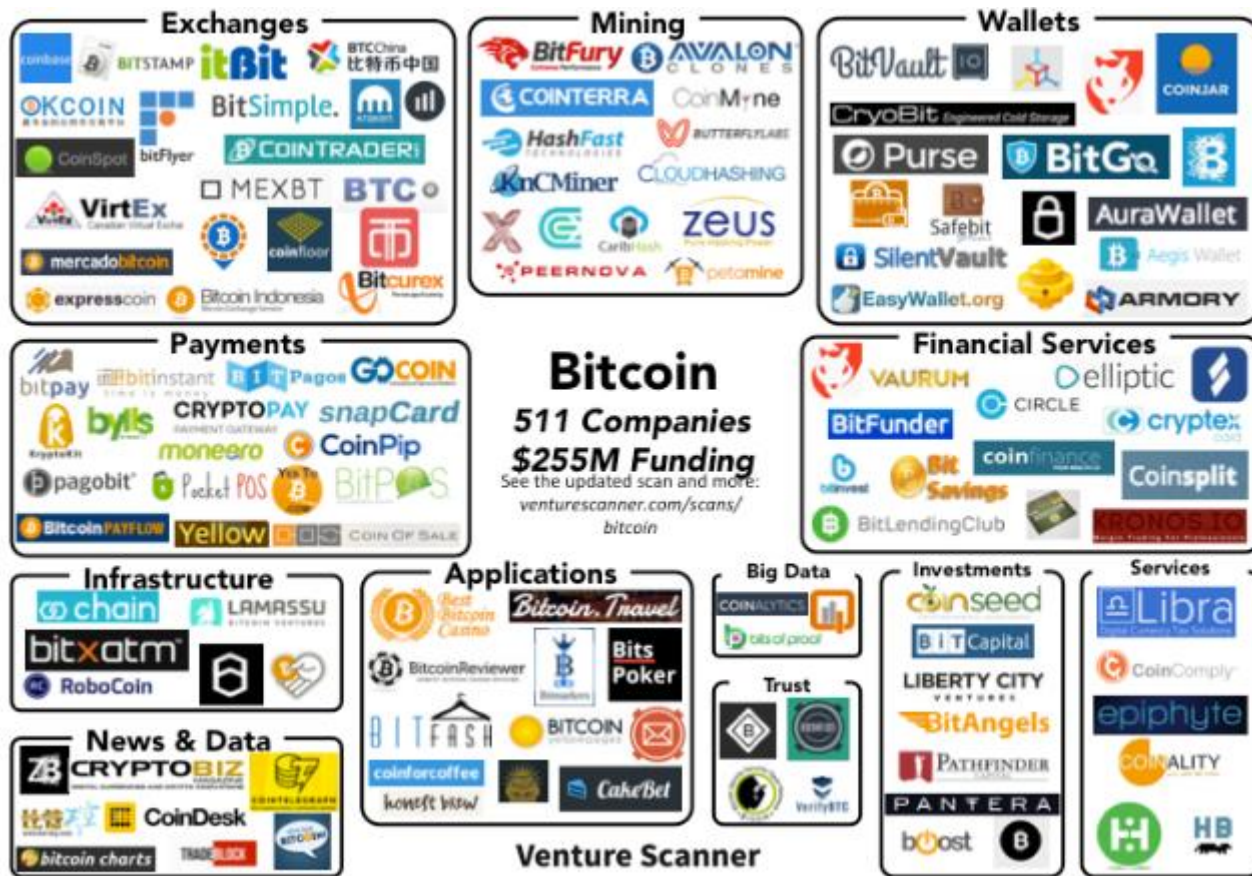


Monero



Ripple

Bitcoin startup



[Source: <https://steemit.com/bitcoin/@cryptolover2017/bitcoin-startup-map>]

CONTENTS

❑ Bank and Blockchain

- “Private blockchain” or “Permissioned ledgers”에 대한 관심
 - ▣ Bitcoin과 같은 인센티브를 부여하는 부분이 없음
 - ▣ No Trustless
 - ▣ Not open
 - ▣ Bitcoin으로부터 “Blockchain”만 분리함

Bank and Blockchain

- 2014.01: Bitcoin을 끊임없이 복제 가능한 가상화폐로 받아들임
 - ▣ 사람들이 여전히 Bitcoin을 이해하지 못함

- 2015.11: Bitcoin 시장 규모가 커지게 될 경우, 규제가 시작될 것.
(아마도 중단될 것)



- “어떤 정부도 통제력이 없는 가상화폐를 원하지 않을 것”

Bank and Blockchain

- 2016.10: JP모건에서 블록체인 자체적으로 도입
- 2017.10: Dimon은 Bitcoin에 대해서 이야기 하지 않고, Bitcoin의 구매가 여전히 어리석다고 여김
- 2018.01: Bitcoin 가격이 \$20,000 에 거래되자, 말을 번복하고, “유감”이라고 말함
- 2019.02: JP모건은 법정 화폐를 나타내는 디지털 코인을 만들고 성공적으로 테스트한 최초의 미국 은행이라고 주장

CONTENTS

- ❑ Blockchain's present and future

Blockchain's present and future

□ 국외

▣ 코인베이스

- 공식 블로그를 통해 탈중앙화 경제를 포괄하는 글로벌 가상자산 앱스토어 구축 계획을 공개 (2021.7.1)

▣ 일론머스크

- 테슬라 및 스페이스X에서도 Bitcoin을 보유중이며, 다시 결제를 지원할 가능성을 언급 (2021.7.22)

▣ 마스터카드

- 신용카드 가맹점에서 사용자가 Bitcoin이나 Ethereum 같은 가상자산으로 결제 요청하면 시스템 내부에서 결제가 이뤄지도록 하는 테스트를 진행중 (2021.7.21)

Blockchain's present and future

□ 국외

▣ 아마존

- '디지털 화폐 및 블록체인 상품 전문가' 채용 공고를 통해 근시 일내에 Bitcoin 결제를 시작하고, 점차 결제에 사용할 수 있는 가상 자산의 종류를 늘려갈 예정 (2021.7.26)

▣ 소프트뱅크

- 소프트뱅크가 브라질 가상자산 거래소 메르카도 비트코인 (Mercado Bitcoin)에 약 2266억원 투자함 (2021.7.2)

Blockchain's present and future

□ 국내

▣ 우리은행

- 디지털 자산 수탁사 '디커스터디'를 설립 및 출범할 예정 (2021.7.11)

▣ NXMH

- 넥슨 지주사인 NXC의 투자 전문 자회사 NXMH가 유럽 암호화폐 거래소 비트스탬프 홀딩스 (Bitstamps Holdings N.V.) 증자에 참여해 2,000억원대를 투자하기로 함 (2021.7.20)

▣ 미래에셋

- 미국에서 암호화폐 상장지수펀드 (ETF)의 출시를 추진 예정 (2021.7.23)

Blockchain's present and future

□ 국내

▣ 국민연금공단

- 한국인터넷진흥원과 함께 '블록체인 기술확산을 위한 업무협약'을 체결 (2021.7.21)

▣ 카카오

- 싱가포르에 블록체인 자회사 설립과 함께 글로벌 시장 진출
- 그라운드X, 클레이(KLAY)

▣ 네이버

- 라인, 링크(LN)을 통한 일본, 동남아시아 중심 블록체인 사업과 국내 가상자산 거래소 빗썸에 가상자산 상장을 통한 국내 시장 공략

- “디지털자산 동향 보고서”, 한국블록체인협회, 2021, 7

Q & A

