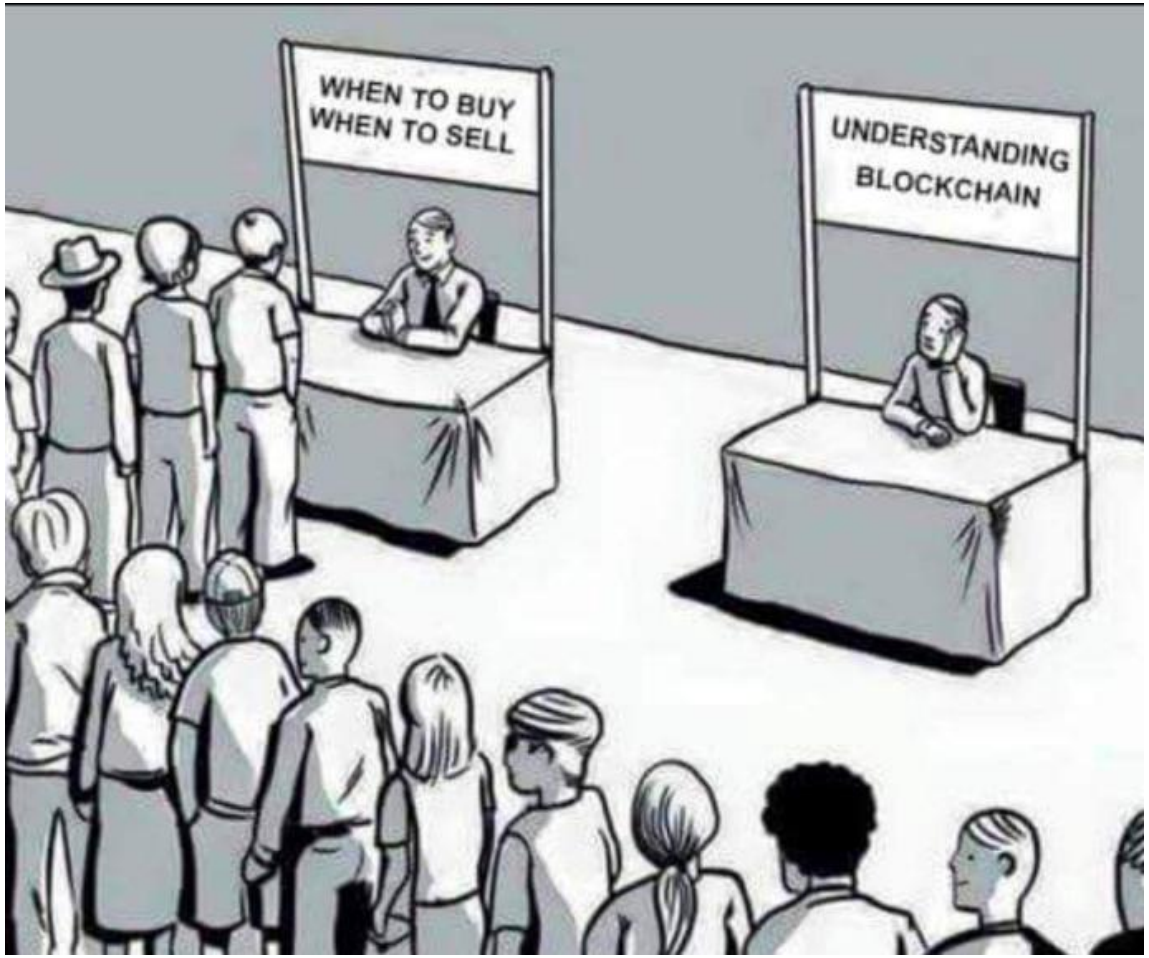
블록체인 개요

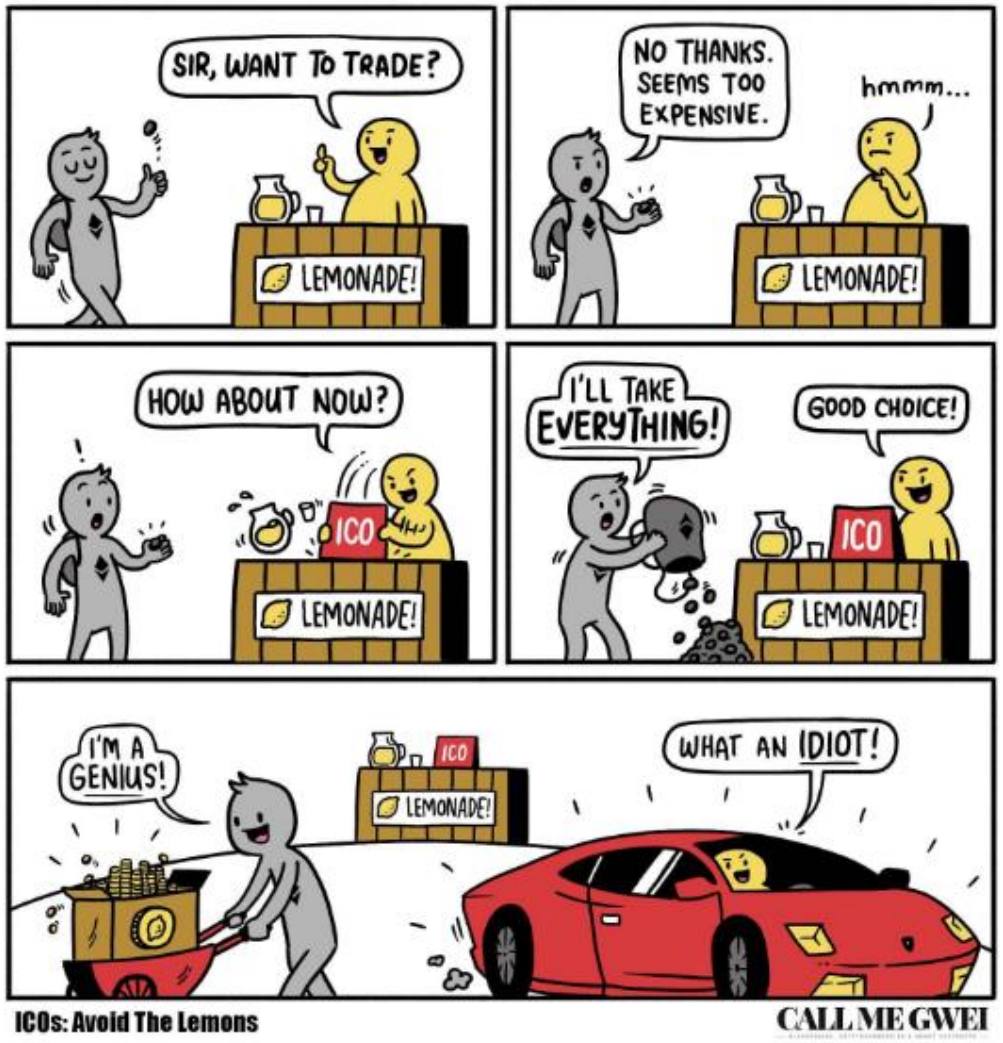
목차

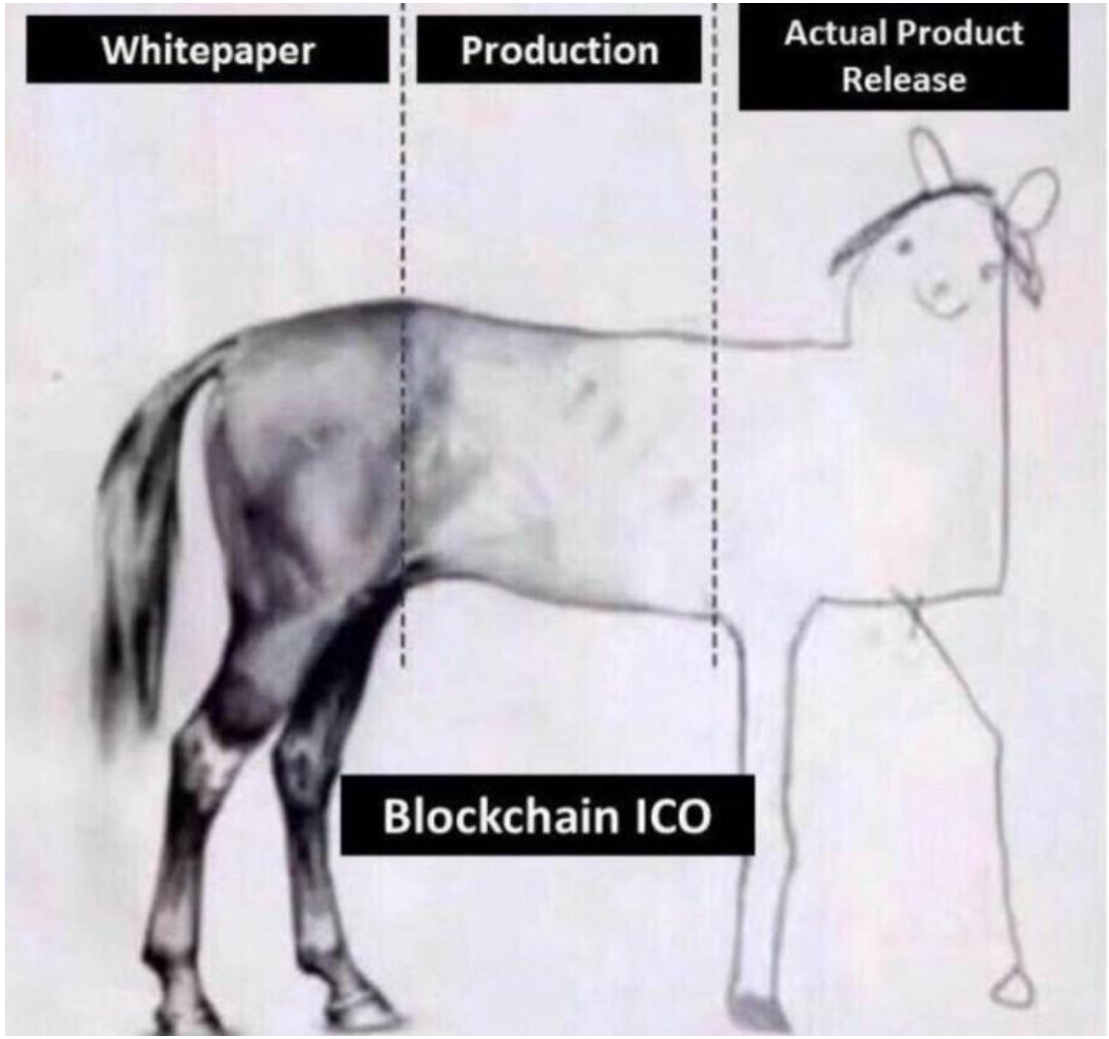
블록체인의 시작


Who thinks blockchain is the future of banking?
Who can explain what blockchain is?


WHEN TO BUY
WHEN TO SELL
UNDERSTANDING
BLOCKCHAIN

블록체인의 시작


SIR, WANT TO TRADE?
LEMONADE!
NO THANKS. SEEMS TOO EXPENSIVE.
hmmm...
LEMONADE!
HOW ABOUT NOW?
ICO
LEMONADE!
I'LL TAKE EVERYTHING!
GOOD CHOICE!
ICO
LEMONADE!
I'M A GENIUS!
ICO
LEMONADE!
WHAT AN IDIOT!
ICOs: Avoid The Lemons
CALL ME GWEI


Whitepaper
Production
Actual Product Release
Blockchain ICO

블록체인의 시작


IT'S A BUBBLE.
IT'S A BUBBLE.
STONETOSS.COM
IT'S A BUBBLE.
IT'S A BUBBLE.


IT'S DOWN 10%: SELL SELL SELL!!!
IT'S DOWN 10%: THINK I'LL BUY MORE

블록체인의 시작

BLIND SIGNATURES FOR UNTRACEABLE PAYMENTS

David Chaum

Department of Computer Science
University of California
Santa Barbara, CA

INTRODUCTION

Automation of the way we pay for goods and services is already underway, as can be seen by the variety and growth of electronic banking services available to consumers. The ultimate structure of

How To Time-Stamp a Digital Document[1]

Stuart Haber and W. Scott Stornetta
Bellcore, 445 South Street,
Morristown, NJ 07960-1910, U.S.A.
stuart@bellcore.com stornetta@bellcore.com

Abstract. The prospect of a world in which all text, audio, picture, and video documents are in digital form on easily modifiable media raises the issue of how to certify when a document was created or last changed. The problem is to time-stamp the data, not the medium. We propose computationally practical procedures for digital time-stamping of such documents so that it is infeasible for

HOW TO MAKE A MINT: THE CRYPTOGRAPHY OF ANONYMOUS ELECTRONIC CASH

Laurie Law, Susan Sabett, Jerry Solinas
National Security Agency Office of Information Security Research and Technology
Cryptology Division
18 June 1996

Untraceable Electronic Cash †
(Extended Abstract)

David Chaum[1] *Amos Fiat*[2] *Moni Naor*[3]

[1] Center for Mathematics and Computer Science
Kruislaan 413, 1098 SJ Amsterdam, The Netherlands
[2] Tel-Aviv University
Tel-Aviv, Israel
[3] IBM Almaden Research Center
650 Harry Road, San Jose, CA 95120

CRYPTO 1988

David Chaum

Formalizing and Securing Relationships on Public Networks

By Nick Szabo

Contents

Introduction
Contracts Embedded in the World
Contemporary Practice
Accounting Controls

Improving the Efficiency and Reliability of Digital Time-Stamping

Dave Bayer*
Barnard College
Columbia University
New York, N.Y. 10027 U.S.A.
dab@math.columbia.edu

Stuart Haber
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stuart@bellcore.com

W. Scott Stornetta
Bellcore
445 South Street
Morristown, N.J. 07960 U.S.A.
stornetta@bellcore.com

March 1992

www.weidai.com/bmoney.txt

I am fascinated by Tim May's crypto-anarchy. Unlike the communities traditionally associated with the word "anarchy", in a crypto-anarchy the government is not temporarily destroyed but permanently forbidden and permanently unnecessary. It's a community where the threat of violence is impotent because violence is impossible, and violence is impossible because its participants cannot be linked to their true names or physical locations.

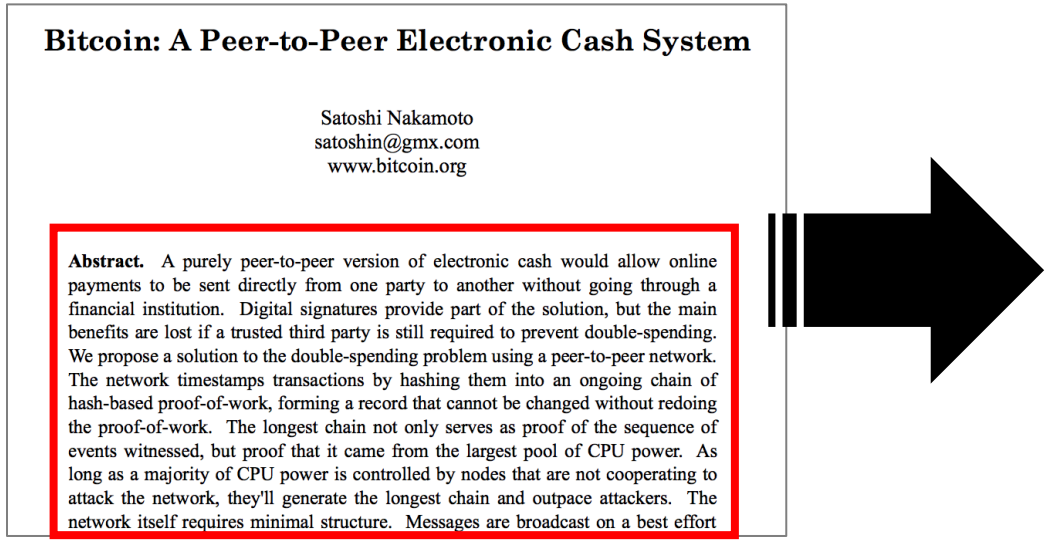
Until now it's not clear, even theoretically, how such a community could operate. A community is defined by the cooperation of its participants, and efficient cooperation requires a medium of exchange (money) and a way to enforce contracts. Traditionally these services have been provided by the government or government sponsored institutions and only to legal entities. In this article I describe a protocol by which these services can be provided to and by untraceable entities.

Saturday, December 27, 2008

Bit gold

A long time ago I hit upon the idea of bit gold. The problem, in a nutshell, is that our money currently depends on trust in a third party for its value. As many inflationary and hyperinflationary episodes during the 20th century demonstrated, this is not an ideal state of affairs. Similarly, private bank note issue, while it had various advantages as well as disadvantages, similarly depended on a trusted third party.

블록체인의 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

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.

순수한 P2P 기반의 전자 화폐는 금융 기관없이 온라인 결제를 직접 할 수 있다

블록체인 정의

데이터의 신뢰성을 확보하는 기술

- 네트워크 내의 참여자가 공동으로 정보 및 가치의 이동을 기록, 검증, 보관, 실행함으로써 중개자 없이도 신뢰 확보가 가능

신뢰를 만드는 기계 (The Trust Machine)

- 서로 믿지 못하는 불특정 다수로 구성된 집단에서 구성원 간의 신뢰를 생성
- 중앙집중 기관이 아닌 참여자들 간의 합의로 운영되는 탈 중앙화
- 거래 내역의 위변조를 방지하여 무결성 보증이 가능

암호화 서명된 트랜잭션들이 블록으로 그룹화된 디지털 원장

- 각 블록을 유효성 확인 후 합의 결정을 거쳐 이전 블록과 암호화된 방식으로 연결되고, 새로운 블록이 추가되면서 이전 블록을 수정하기 어려워짐

트랜잭션의 그룹으로 구성된 블록의 연결 리스트

- 일관성, 불변성, 소유가능성, 탈중앙성, 표준화, 속성이 추가된 데이터베이스의 하위 집합

블록체인 정의

블록체인 정의

경제적 측면

사회적 측면

기술적 측면

경제 - 돈이 되는 무언가

10년간 가장 고수익 투자는 '비트코인'...9만배 뛰었다

뉴스1 입력 2019-12-18 11:38 수정 2019-12-18 11:38

롤러코스터 타는 비트코인…하루만에 8% ↑

김수찬 기자 | 입력 2019-12-19 09:55

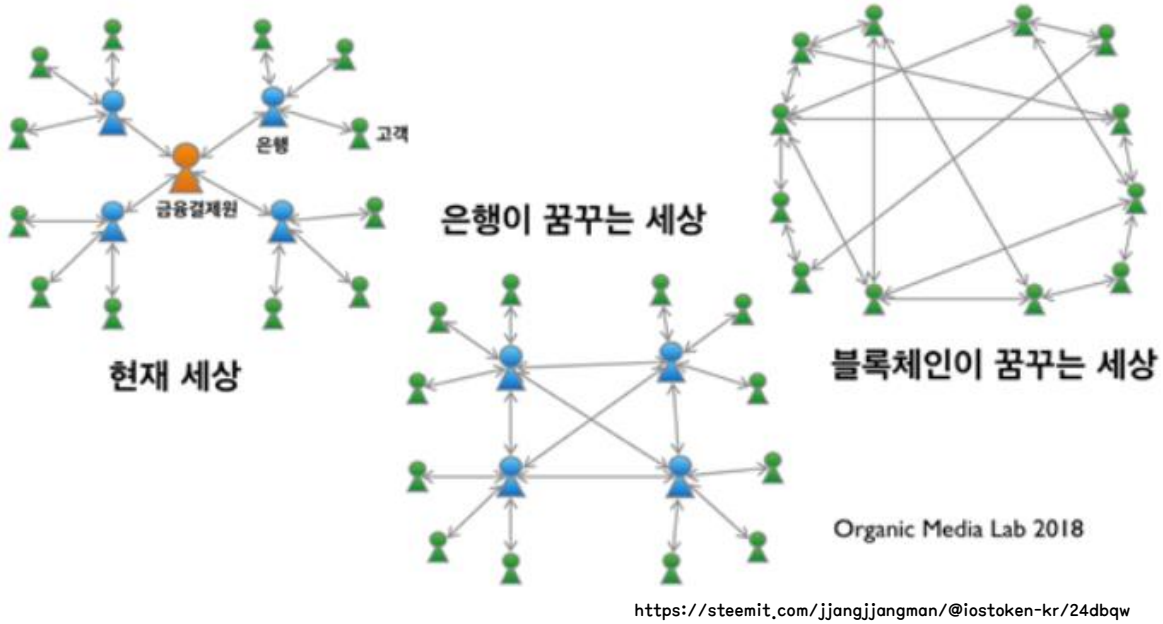
[가상화폐] 18일 오전 9시 30분 비트코인 7,764,000원(+0.28%) 거래중

입력 2019.12.18 09:31 | 수정 2019.12.18 09:31

1000만원 찍은 비트코인, 어디까지 갈까 팽팽한 전망

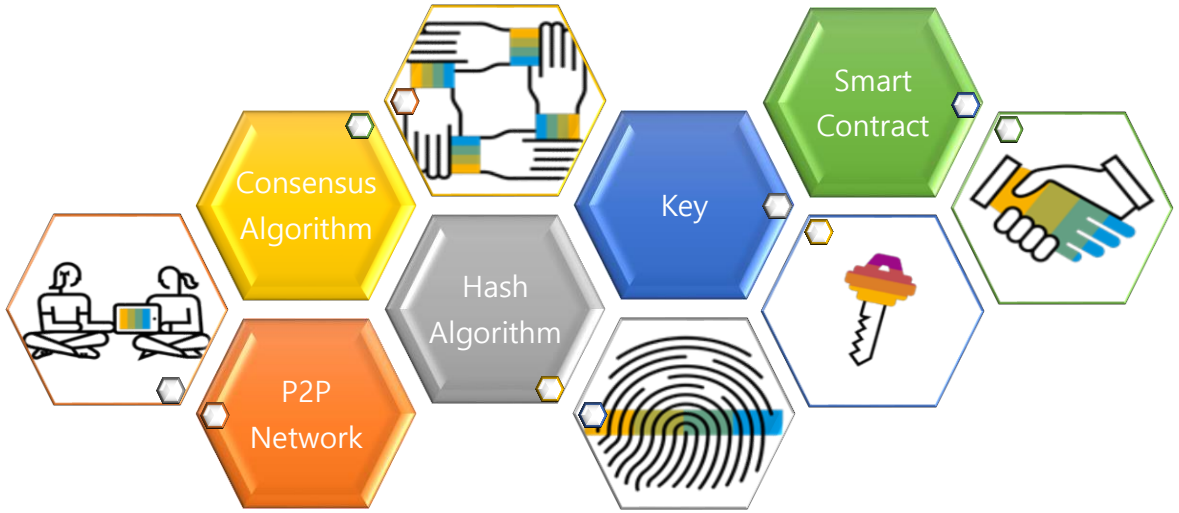
비트코인 가격, 사상 최고치 기록 등...2019년 암호화폐 전망은?

사회 – 현실을 바꿔줄 무언가



https://steemit.com/jjangjjangman/@iostoken-kr/24dbqw

기술 – 혼합된 무언가


Consensus Algorithm
Hash Algorithm
Key
Smart Contract
P2P Network

1. 블록체인의 탄생

1) 블록체인의 시작
2) 블록체인 정의

2. 블록체인 기술적 요소

1) P2P Network
2) Hash Algorithm
3) Key
4) Consensus Algorithm
5) Smart Contract

3. 블록체인 플랫폼

1) 비트코인
2) 이더리움
3) 하이퍼레저 페브릭
4) 하이퍼레저 베수
5) 클레이튼

4. 블록체인 동향

1) 블록체인과 지갑
2) 블록체인과 DApp
3) NFT와 블록체인
4) 메타버스와 블록체인
5) WEB 3.0과 블록체인

P2P Network

www가 나올당시
컴퓨터 간의 연결을 목적으로
했기 때문에 P2P와 유사

1999년 napster를 통한
첫 File sharing 서비스

완전한 P2P 보다는
파일을 서버에 올리고
파일을 서버가 확인 후
다른 사람에게 전송

그누텔라 (비 공개형 P2P)

통신해야하는 상대방 IP
주소를 알고 있어야 통신 가능

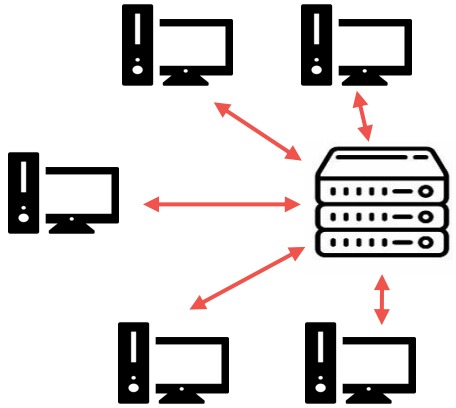
당나귀 (공개형 P2P)

파일 분할식 공유
최초로 대용량 공유가 가능함

토렌트
(공개형 P2P &
비 공개형 P2P)

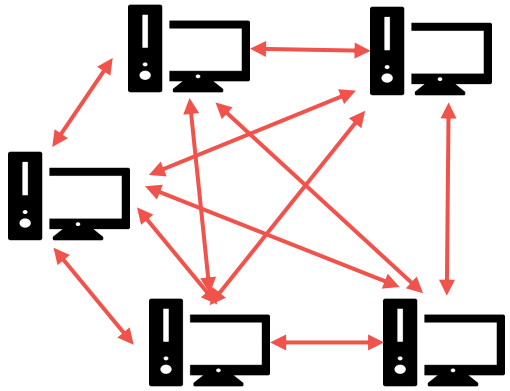
P2P Network

클라이언트 & 서버



- 서버를 통해서 모든 통신이 이루어짐
- 유지 보수가 쉬움
- 보안을 유지가 쉬움
- 서버에 네트워크 트래픽이 집중됨

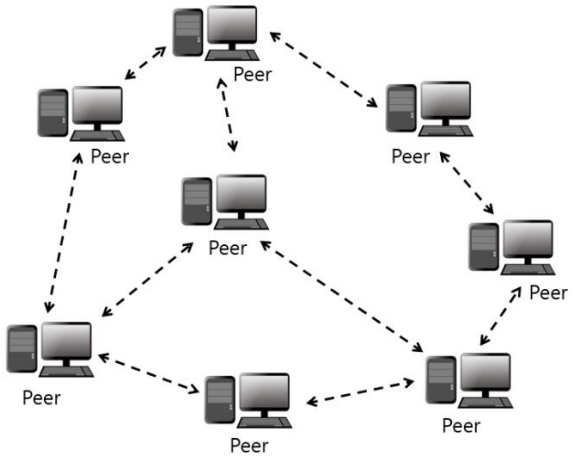
P2P



- 트래픽을 분산 시킬 수 있음
- 새로운 기능 추가, 업데이트가 어려움

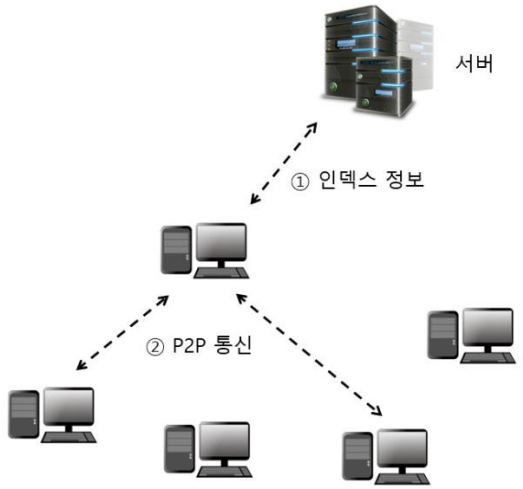
P2P Network

Pure P2P



- 모든 노드가 동등한 입장
- 새로운 노드의 추가가 쉬움

Hybrid P2P

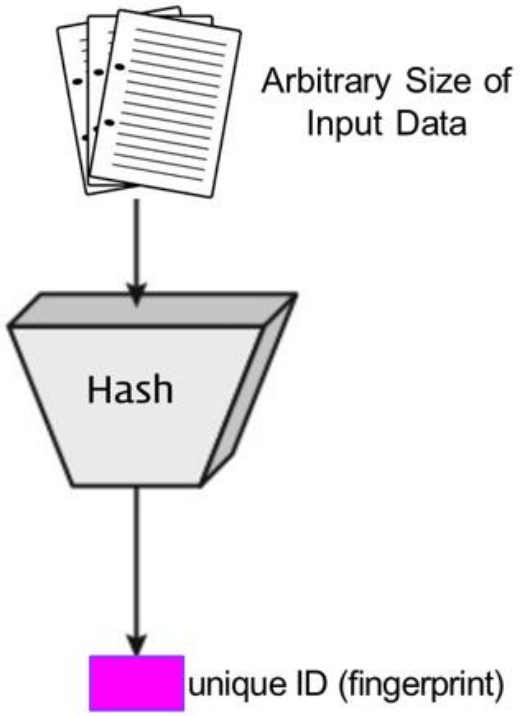


- 각 노드들의 정보가 인덱스 서버에 기록
- 노드간의 데이터는 P2P 통신으로 이루어지나 탐색 및 발견은 인덱스 서버를 통해 이루어짐

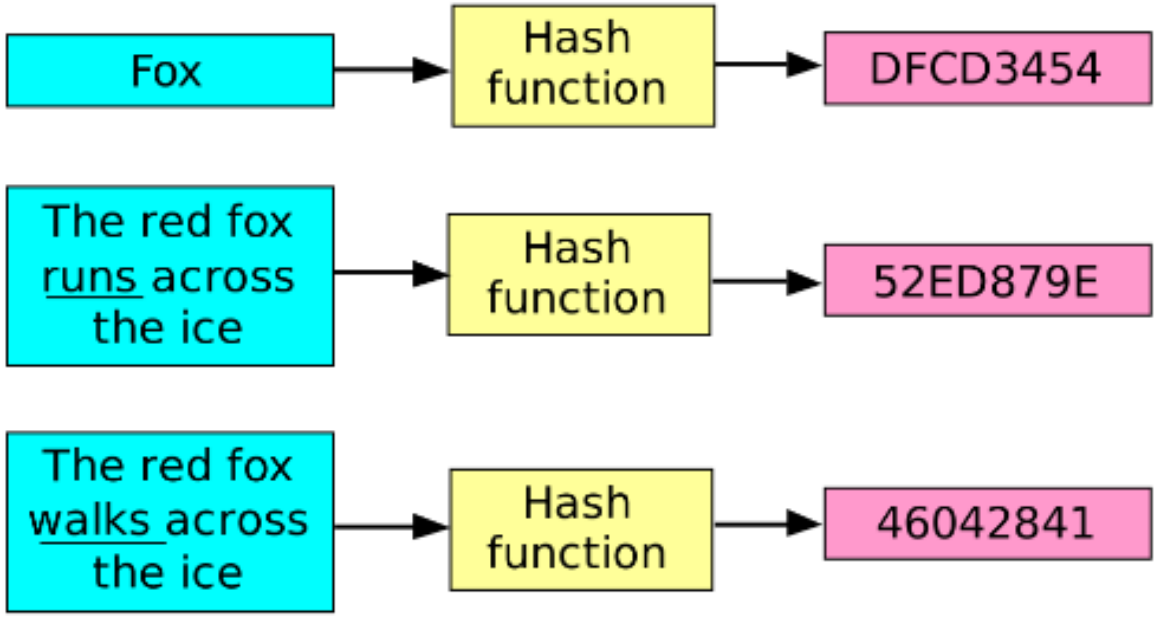
Hash Algorithm

- 고정 크기의 출력
  - 임의의 입력, 고정 크기의 출력

- 문서나 파일의 손상 여부를 검증하는 데에 사용
- 복제물은 원본과 같은 지 여부를 검증
  - 두 문서의 글자를 모두 비교할 필요가 없음
  - 두 파일의 해시값만 비교로 충분

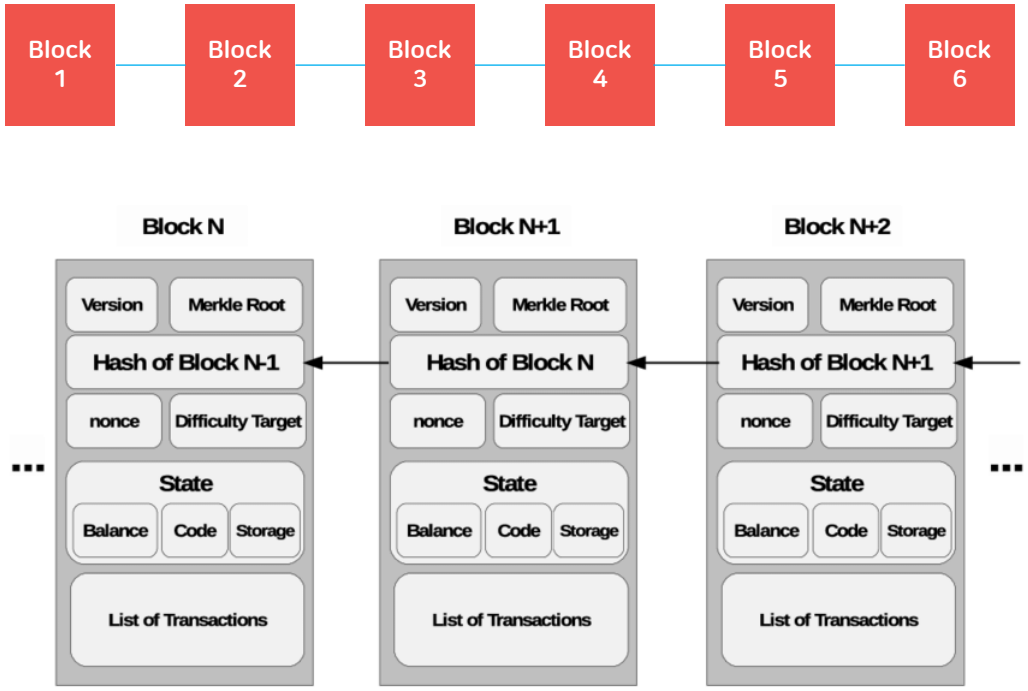


Hash Algorithm



- 해시 함수란 임의의 길이를 갖는 데이터를 고정된 길이를 가진 해시 값으로 바꿔주는 함수

Hash Algorithm



https://www.researchgate.net/figure/Blockchain-design-structure-showing-chained-blocks-with-header-and-body-fields_fig2_321017113

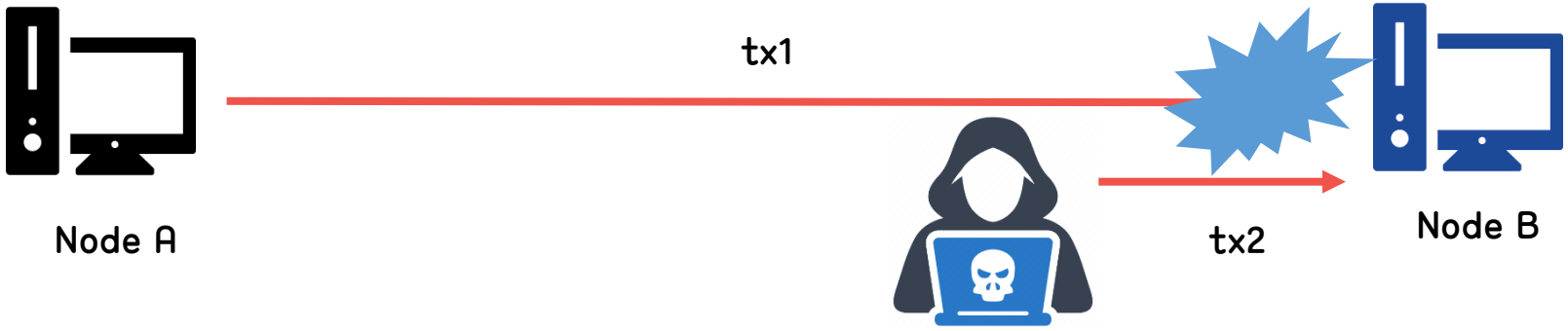
블록체인에서 Hash Algorithm은

1) 데이터의 간결하게 표현

2) 데이터의 무결성을 검증

3) Proof of Work에 사용

Key



키가 없는 경우 누가 메시지를 보냈는지 모름

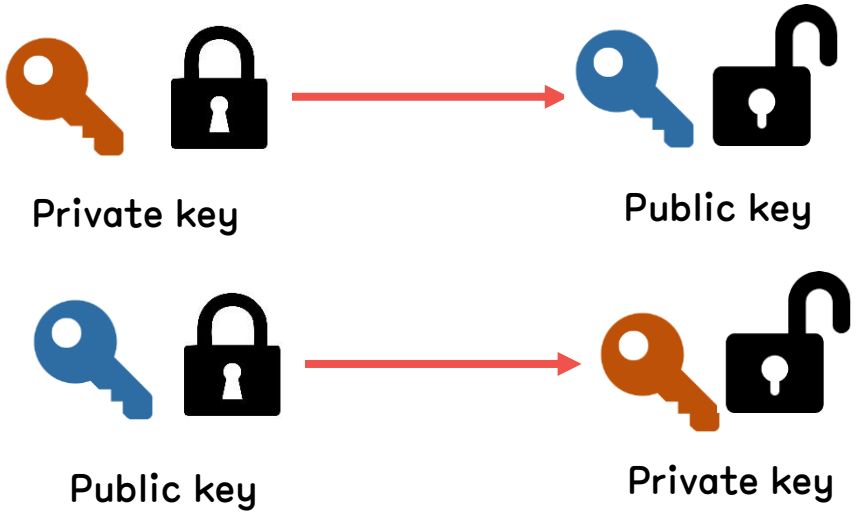
Key

대칭키

- 하나의 키로 암호화 복호화를 진행
- 속도가 빠름

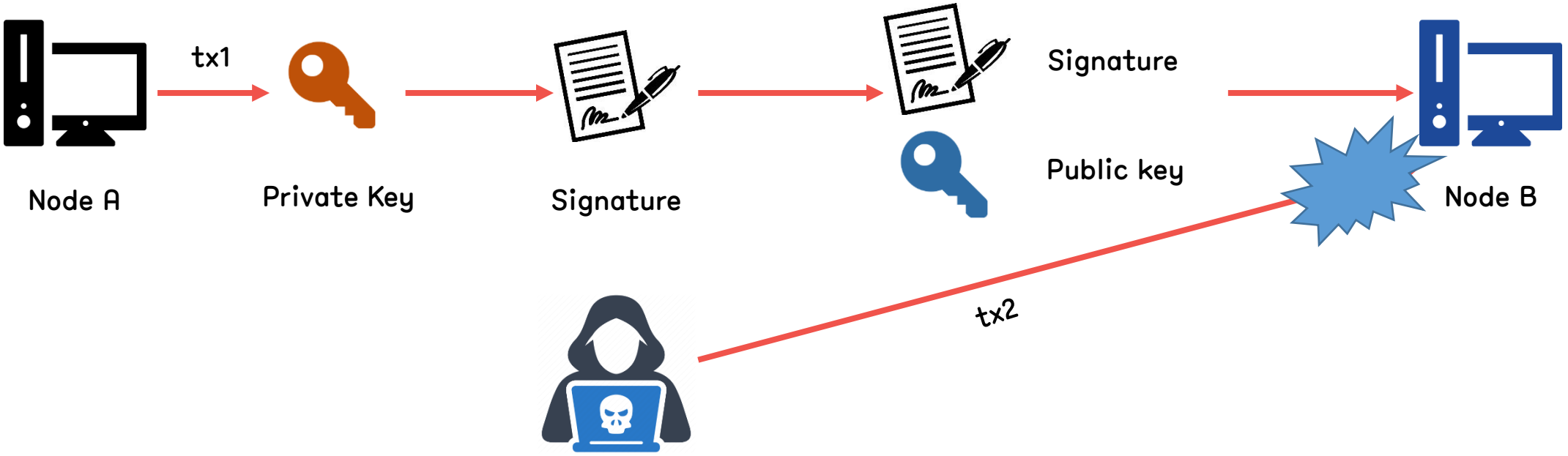
비 대칭키

- Public Key와 Private Key가 존재



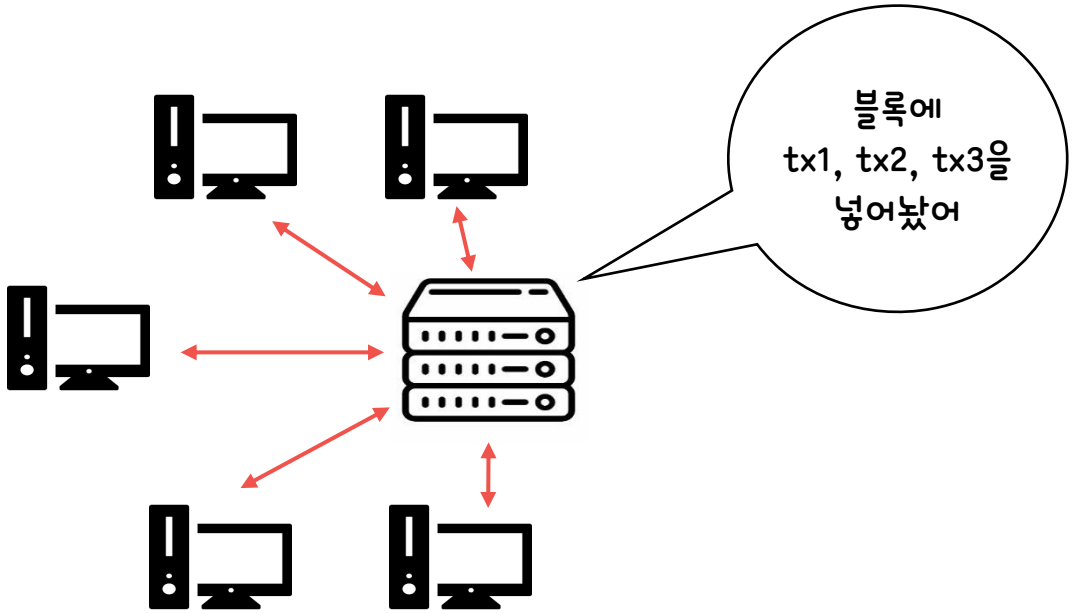
전자서명

데이터의 출처를 밝히기 위해서 Key를 사용

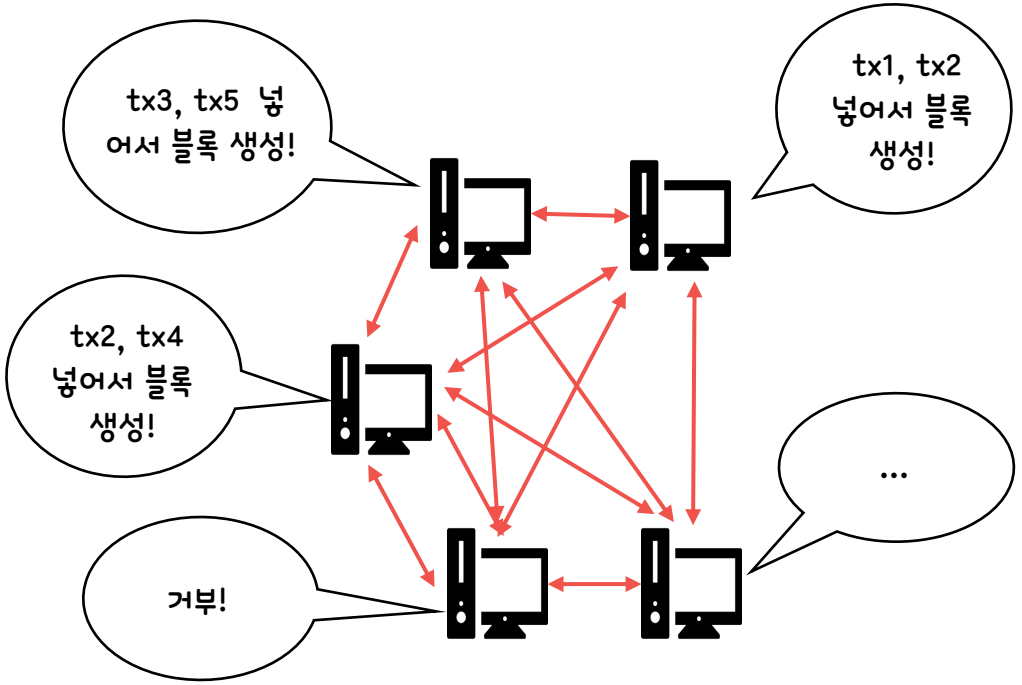


Consensus Algorithm

클라이언트 & 서버 구조



P2P 구조



Consensus Algorithm

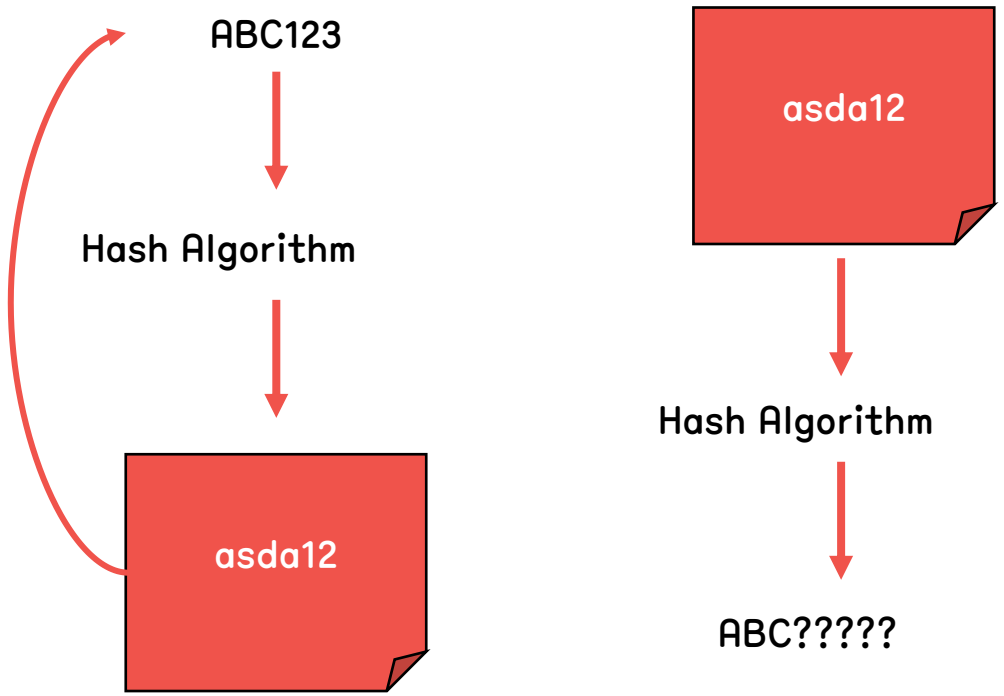
리더 선출

- Proof of XXX
- 특정 알고리즘을 통해 리더를 선출 후, 대표자가 블록을 생성
- Proof of Work, Proof of Stake

투표

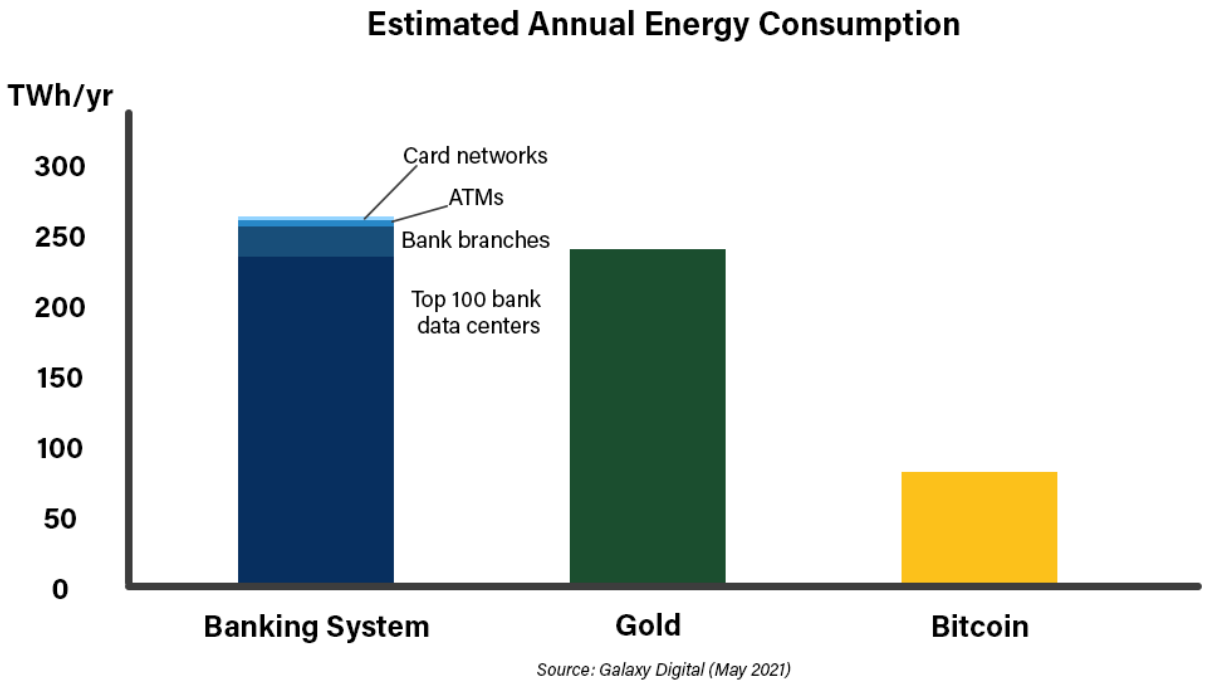
- 모든 노드가 참여하여, 투표를 진행
- 블록을 제시하는 리더가 존재
- PBFT, DPoS, Tendermint

작업증명 (PoW: Proof of Work)



- 특정 Hash 함수를 주고, Input값을 맞추는 과정
- Input값을 가장 빨리 맞추는 사람이 블록 생성 권한을 가짐
- Computer Resource를 많이 쓰는 노드
  = 일을 많이 한 노드 = 정직한 노드
- Computer Resource 낭비가 심함

Consensus Algorithm

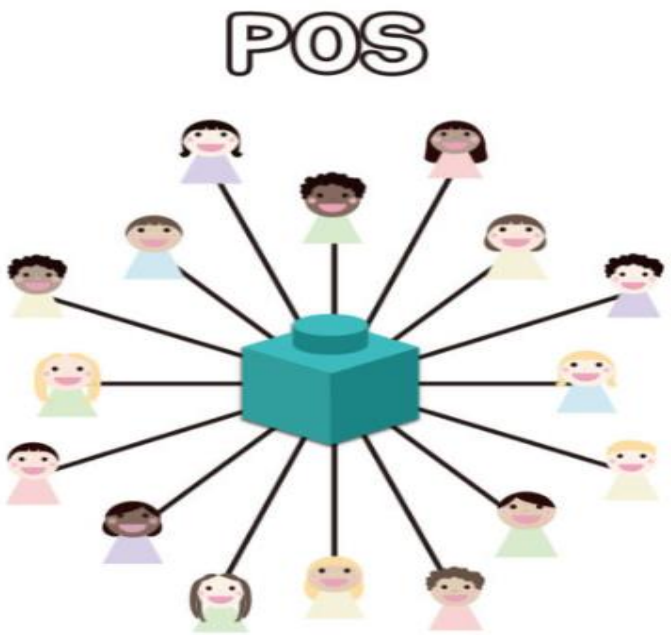


홈 > 한경BUSINESS

비트코인 채굴이 환경 오염 주범?...세계 전력 소비 0.66% 불과[비트코인 A to Z]

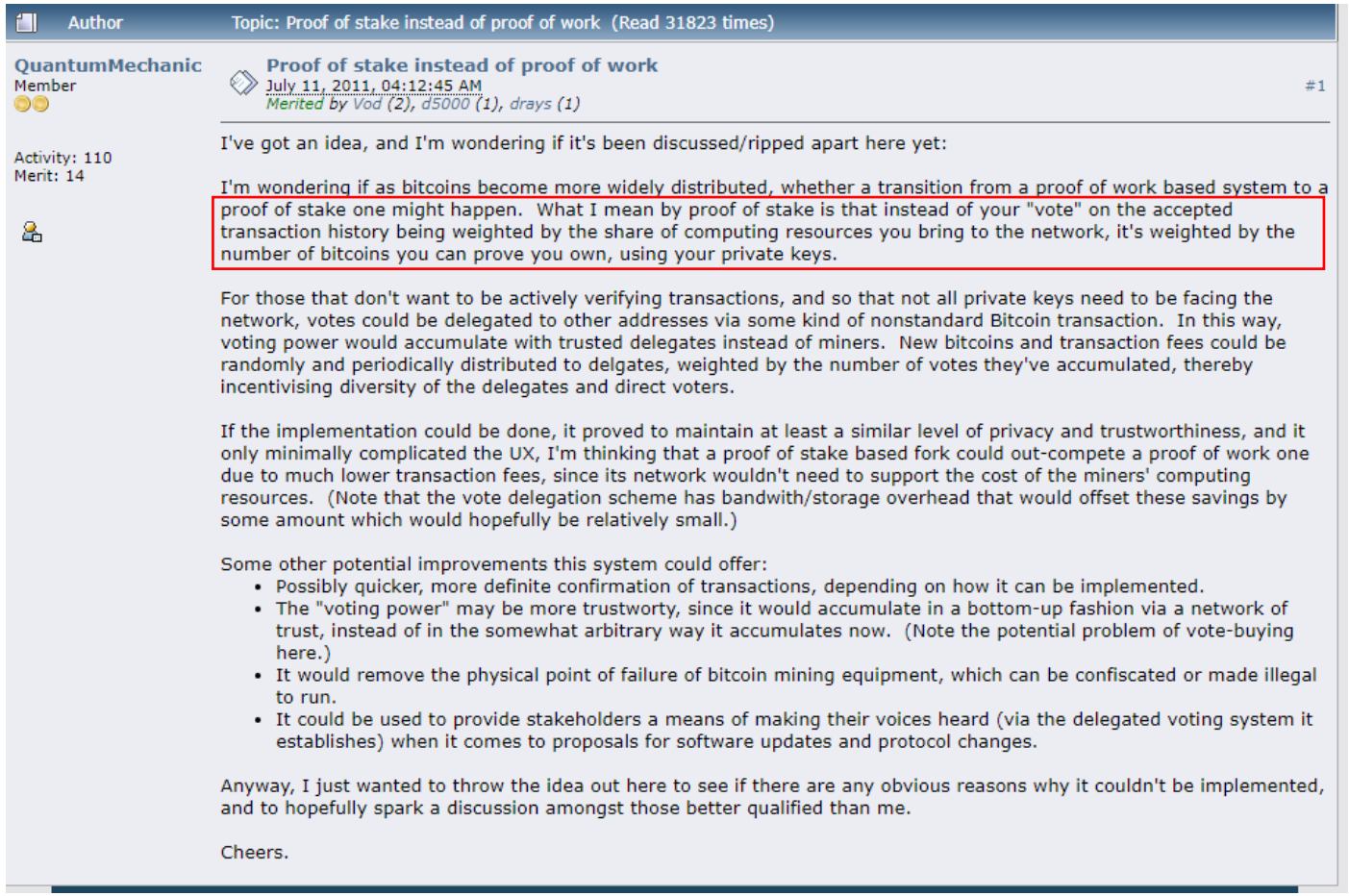
입력 2021.05.25 06:54 | 수정 2021.05.25 06:54

지분증명 (PoS; Proof of Stake)



- 작업 증명의 한계를 해결하기 위해서 만들어짐
- 지분에 따라서 블록 생성 권한을 주는 방식
- 대부분이 Coin Age 방식을 사용 하고 있음
- 다른합의알고리즘과 융합하여 사용하는 형태
- 블록생성의 중앙화 문제가 있음

Consensus Algorithm



Author | Topic: Proof of stake instead of proof of work (Read 31823 times)

QuantumMechanic
Member

Activity: 110
Merit: 14

Proof of stake instead of proof of work
July 11, 2011, 04:12:45 AM #1
Merited by Vod (2), d5000 (1), drays (1)

I've got an idea, and I'm wondering if it's been discussed/ripped apart here yet:

I'm wondering if as bitcoins become more widely distributed, whether a transition from a proof of work based system to a proof of stake one might happen. What I mean by proof of stake is that instead of your "vote" on the accepted transaction history being weighted by the share of computing resources you bring to the network, it's weighted by the number of bitcoins you can prove you own, using your private keys.

For those that don't want to be actively verifying transactions, and so that not all private keys need to be facing the network, votes could be delegated to other addresses via some kind of nonstandard Bitcoin transaction. In this way, voting power would accumulate with trusted delegates instead of miners. New bitcoins and transaction fees could be randomly and periodically distributed to delgates, weighted by the number of votes they've accumulated, thereby incentivising diversity of the delegates and direct voters.

If the implementation could be done, it proved to maintain at least a similar level of privacy and trustworthiness, and it only minimally complicated the UX, I'm thinking that a proof of stake based fork could out-compete a proof of work one due to much lower transaction fees, since its network wouldn't need to support the cost of the miners' computing resources. (Note that the vote delegation scheme has bandwith/storage overhead that would offset these savings by some amount which would hopefully be relatively small.)

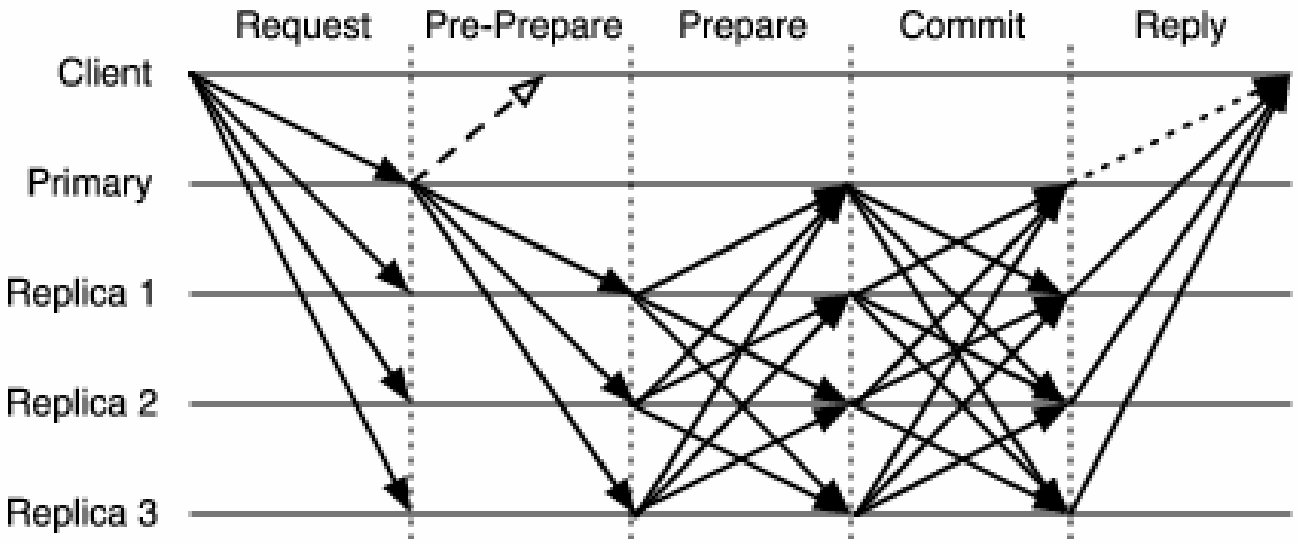
Some other potential improvements this system could offer:

- Possibly quicker, more definite confirmation of transactions, depending on how it can be implemented.
- The "voting power" may be more trustworty, since it would accumulate in a bottom-up fashion via a network of trust, instead of in the somewhat arbitrary way it accumulates now. (Note the potential problem of vote-buying here.)
- It would remove the physical point of failure of bitcoin mining equipment, which can be confiscated or made illegal to run.
- It could be used to provide stakeholders a means of making their voices heard (via the delegated voting system it establishes) when it comes to proposals for software updates and protocol changes.

Anyway, I just wanted to throw the idea out here to see if there are any obvious reasons why it couldn't be implemented, and to hopefully spark a discussion amongst those better qualified than me.

Cheers.

실용적 비잔틴 장애 허용 (PBFT; Practical Byzantine Fault Tolerance)

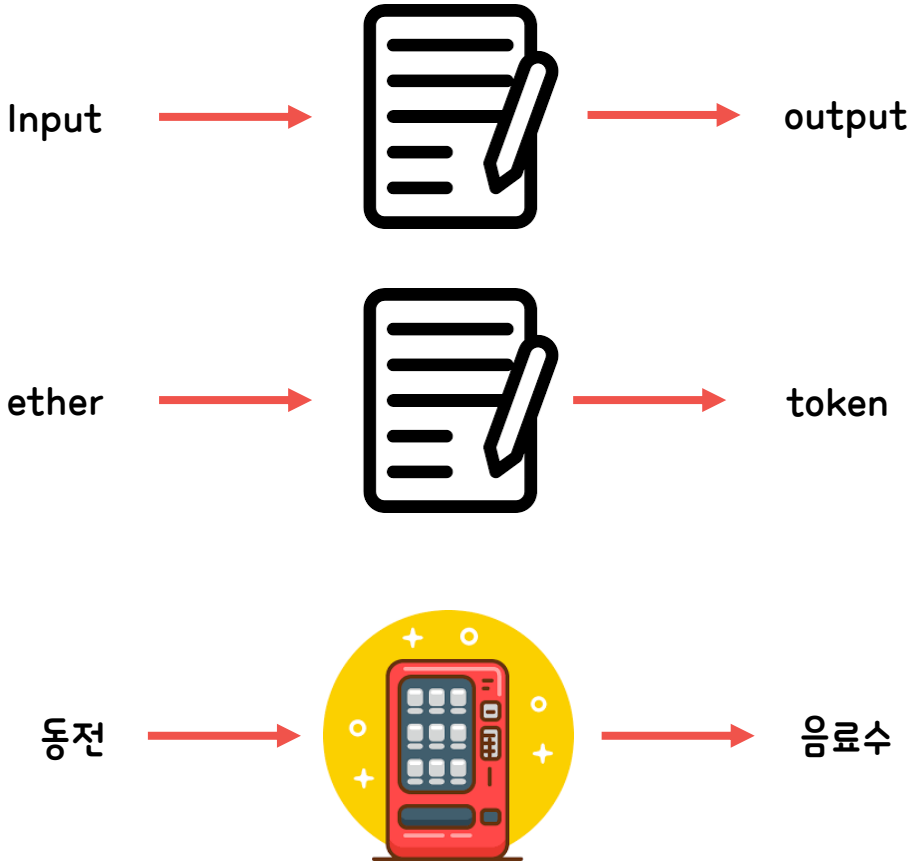


- 클라이언트가 블록을 제시 하고 해당 블록에 대해서 매번 투표를 진행 하는 방식
- 데이터의 안전성을 보장
- 노드 수가 많아질수록 합의에 도달하는 시간이 오래 걸림

Smart Contract

- 1994년 Nick Szabo가 제시한 개념
- 디지털화된 계약서가 해킹될 경우 문제가 발생
- 이더리움을 통해 스마트컨트렉트가 사용됨
- 코드의 조각
- 블록체인과 상호 작용하는 인터페이스

Smart Contract



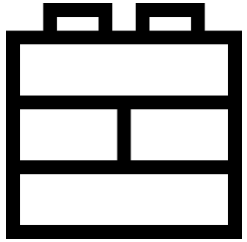
Smart Contract

스마트 컨트렉트
생성

컴파일

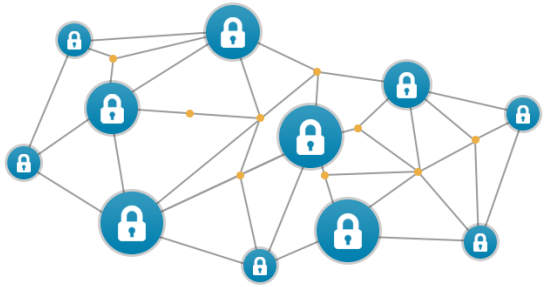
바이트 코드 변환

트랜잭션



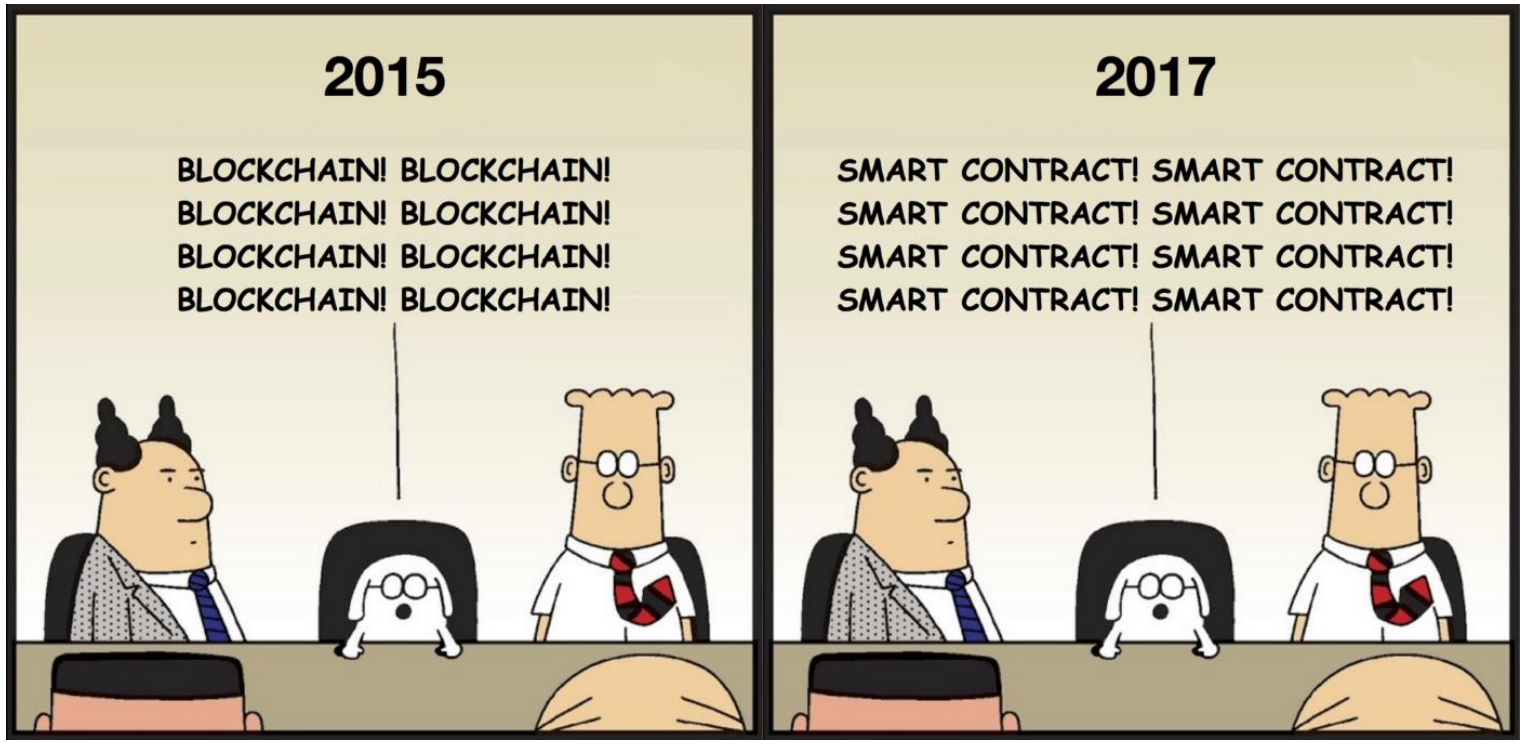
블록에 저장

배포



블록체인에 저장

Smart Contract



https://hakin9.org/the-truth-about-smart-co

1. 블록체인의 탄생

1) 블록체인의 시작
2) 블록체인 정의

2. 블록체인 기술적 요소

1) P2P Network
2) Hash Algorithm
3) Key
4) Consensus Algorithm
5) Smart Contract

3. 블록체인 플랫폼

1) 비트코인
2) 이더리움
3) 하이퍼레저 페브릭
4) 하이퍼레저 베수
5) 클레이튼

4. 블록체인 동향

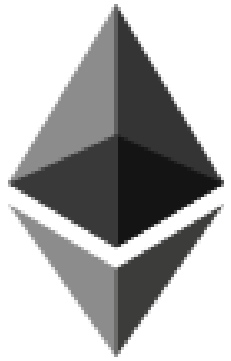
1) 블록체인과 지갑
2) 블록체인과 DApp
3) NFT와 블록체인
4) 메타버스와 블록체인
5) WEB 3.0과 블록체인

비트코인

비트코인(bitcoin)은 블록체인 기술을 기반으로 만들어진 온라인 암호화폐이다. 비트코인의 화폐 단위는 BTC 또는 XBT로 표시한다. 2008년 10월 사토시 나카모토라는 가명을 쓰는 프로그래머가 개발하여, 2009년 1월 프로그램 소스를 배포했다. 중앙은행이 없이 전 세계적 범위에서 P2P 방식으로 개인들 간에 자유롭게 송금 등의 금융거래를 할 수 있게 설계되어 있다. 거래장부는 블록체인 기술을 바탕으로 전 세계적인 범위에서 여러 사용자들의 서버에 분산하여 저장하기 때문에 해킹이 사실상 불가능하다. SHA-256 기반의 암호 해시 함수를 사용한다.

https://ko.wikipedia.org/wiki/%EB%B9%84%ED%8A%B8%EC%BD%94%EC%9D%B8

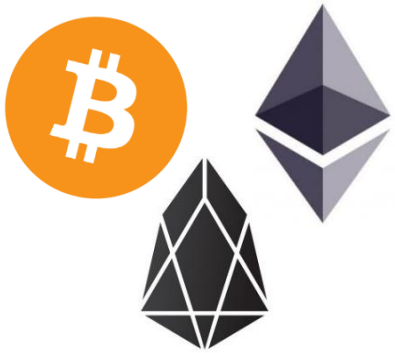
이더리움



이더리움(Ethereum)은 블록체인 기술을 기반으로 스마트 계약 기능을 구현하기 위한 분산 컴퓨팅 플랫폼이다. 이더리움이 제공하는 이더(Ether)는 비트코인과 마찬가지로 암호화폐의 일종으로 거래되고 있다. 이더리움의 화폐 단위는 ETH로 표시한다. 비트코인 이후에 등장한 알트코인 중 시가 총액이 가장 높은 대표적인 알트코인이다. Ethereum의 정확한 발음은 미국식으로는 이씨리엄([iˈθɪɹiəm])[2]이고, 영국식으로는 이씨어리엄([iˈθɪəɹiəm])[3]이다. 이더리움은 초기에 '이시리움' 또는 '에테리움'이라고 표기하기도 하였으나, 요즘에는 '이더리움'으로 표기하는 경우가 많다.

https://ko.wikipedia.org/wiki/%EC%9D%B4%EB%8D%94%EB%A6%AC%EC%9B%80

하이퍼레저 페브릭



퍼블릭 블록체인

- 네트워크 누구나 참여 가능

프라이빗 블록체인

- 허가받은 사용자만 참여 가능

하이퍼레저 페브릭

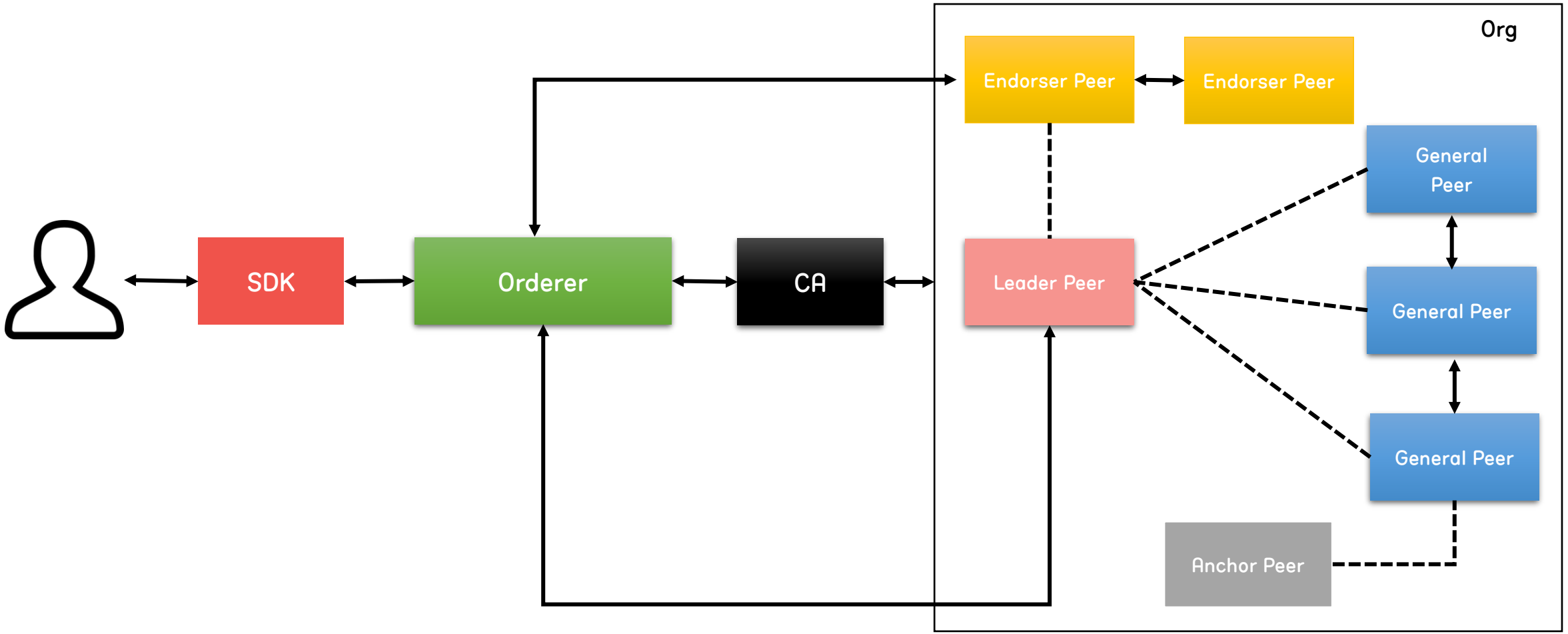
- IBM이 주도하는 프로젝트
- 프라이빗 블록체인에서 가장 유명함
- 접근 제어 기능을 제공

- DID 제공 플랫폼

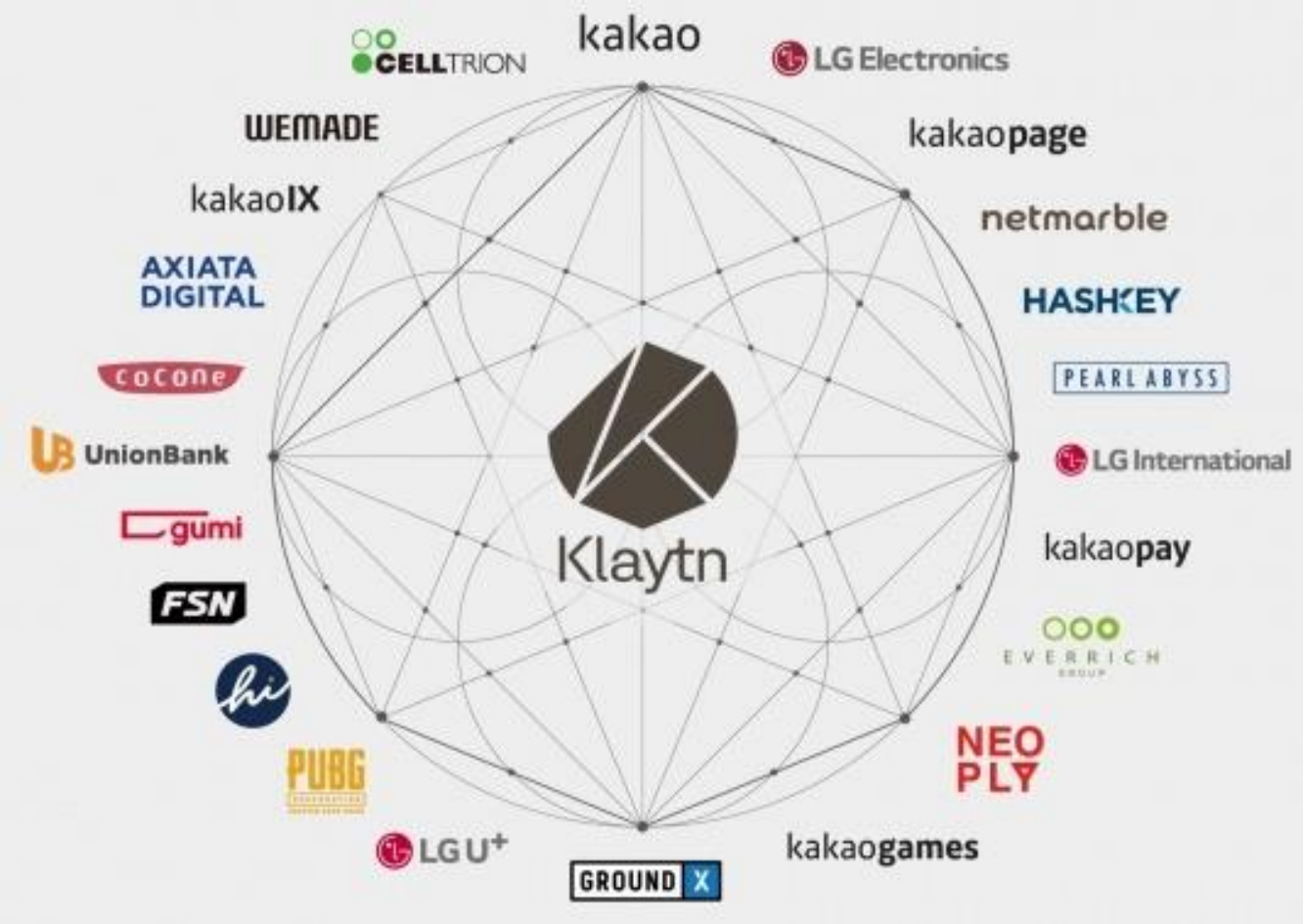
- Intel이 주도하는 프로젝트
- IoT 환경에서의 블록체인

- 이더리움 프라이빗 네트워크

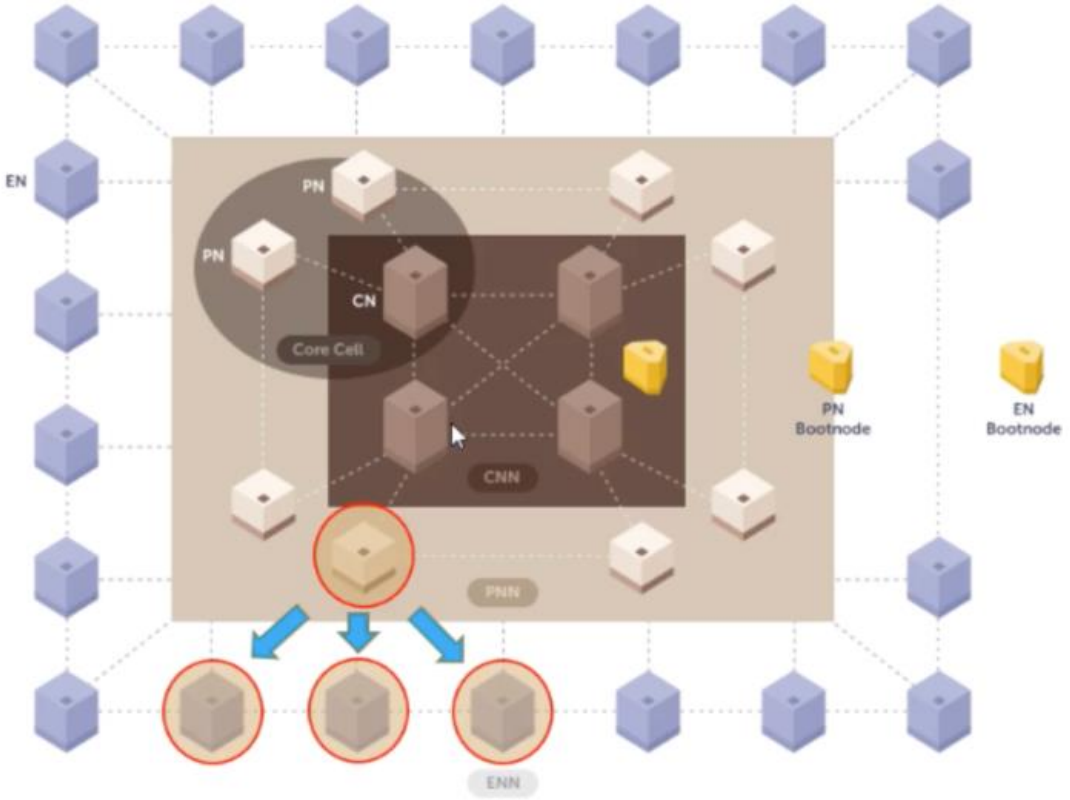
하이퍼레저 페브릭


Org
Endorser Peer
Endorser Peer
General Peer
SDK
Orderer
CA
Leader Peer
General Peer
General Peer
Anchor Peer

클레이튼


kakao
CELLTRION
LG Electronics
WEMADE
kakaopage
kakaoIX
netmarble
AXIATA DIGITAL
HASHKEY
cocone
PEARL ABYSS
UnionBank
LG International
gumi
kakaopay
FSN
EVERRICH
hi
NEO PLY
PUBG
LG U+
kakaogames
GROUND X
Klaytn

클레이튼



- CN
  - 합의를 진행하는 노드
- PN
  - 외부 EN으로 부터 받은 트랜잭션을 CN에 전달
- EN
  - 서비스 사용자 노드

1. 블록체인의 탄생

1) 블록체인의 시작
2) 블록체인 정의

2. 블록체인 기술적 요소

1) P2P Network
2) Hash Algorithm
3) Key
4) Consensus Algorithm
5) Smart Contract

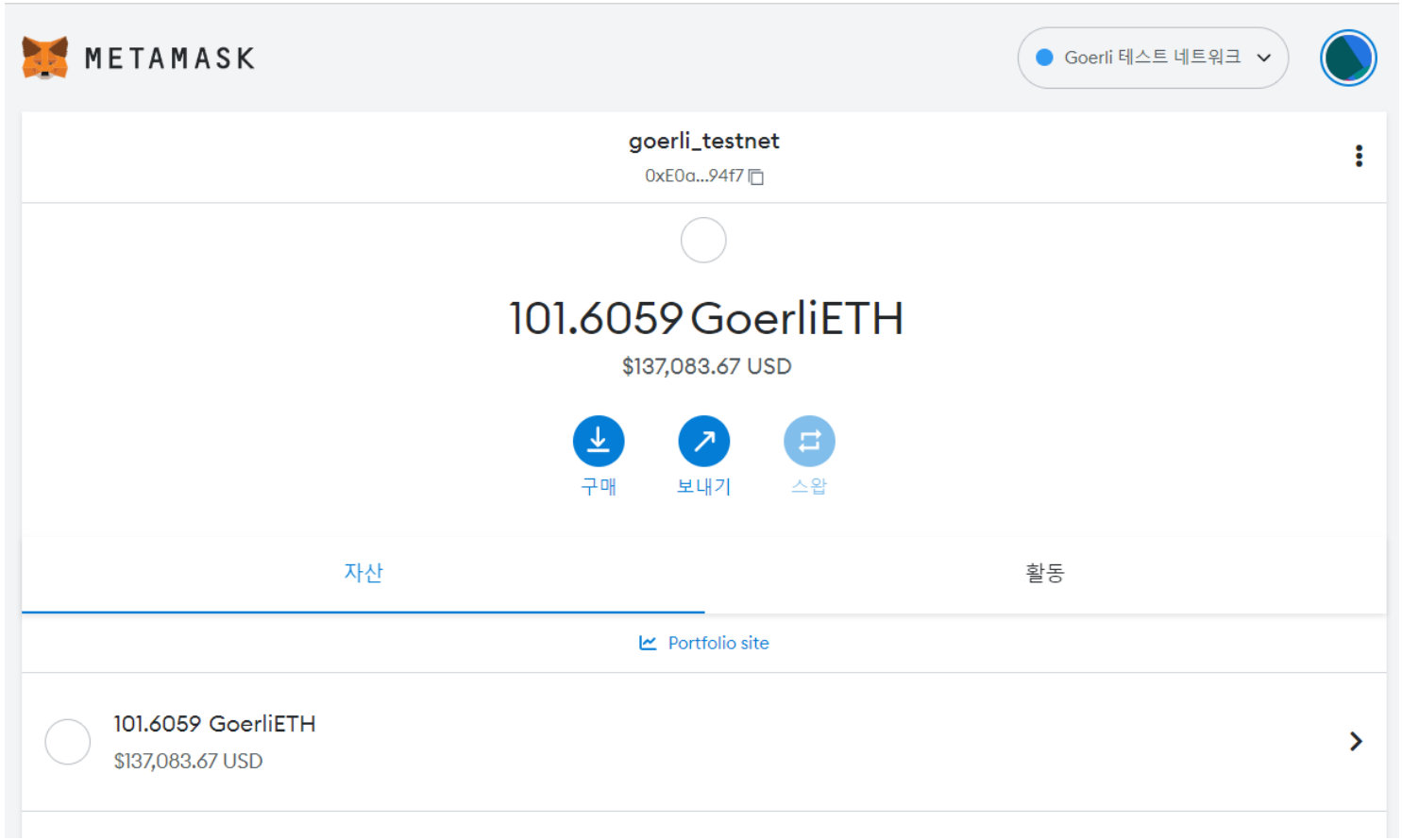
3. 블록체인 플랫폼

1) 비트코인
2) 이더리움
3) 하이퍼레저 페브릭
4) 하이퍼레저 베수
5) 클레이튼

4. 블록체인 동향

1) 블록체인과 지갑
2) 블록체인과 DApp
3) CBDC
4) NFT와 블록체인
5) 메타버스와 블록체인
6) WEB 3.0과 블록체인

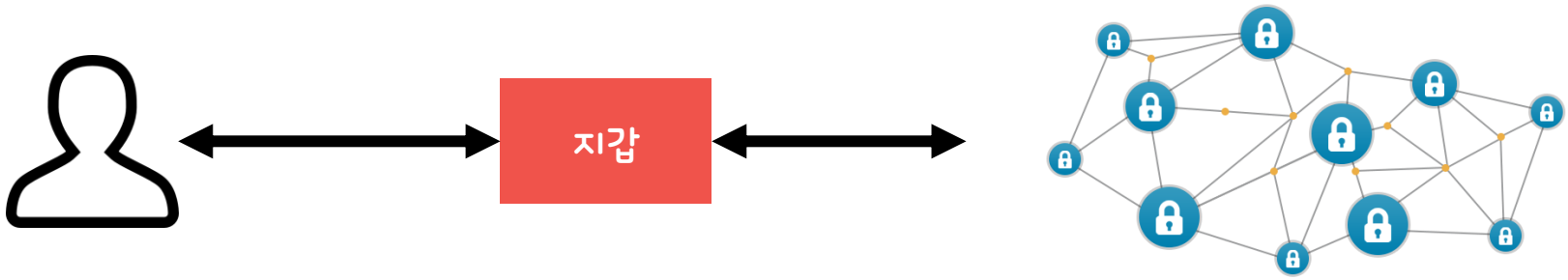
블록체인 지갑



- 지갑은 블록체인 인가?
- 지갑은 왜 필요한가?
- 지갑의 중요성

블록체인 지갑

지갑은 블록체인 인가?

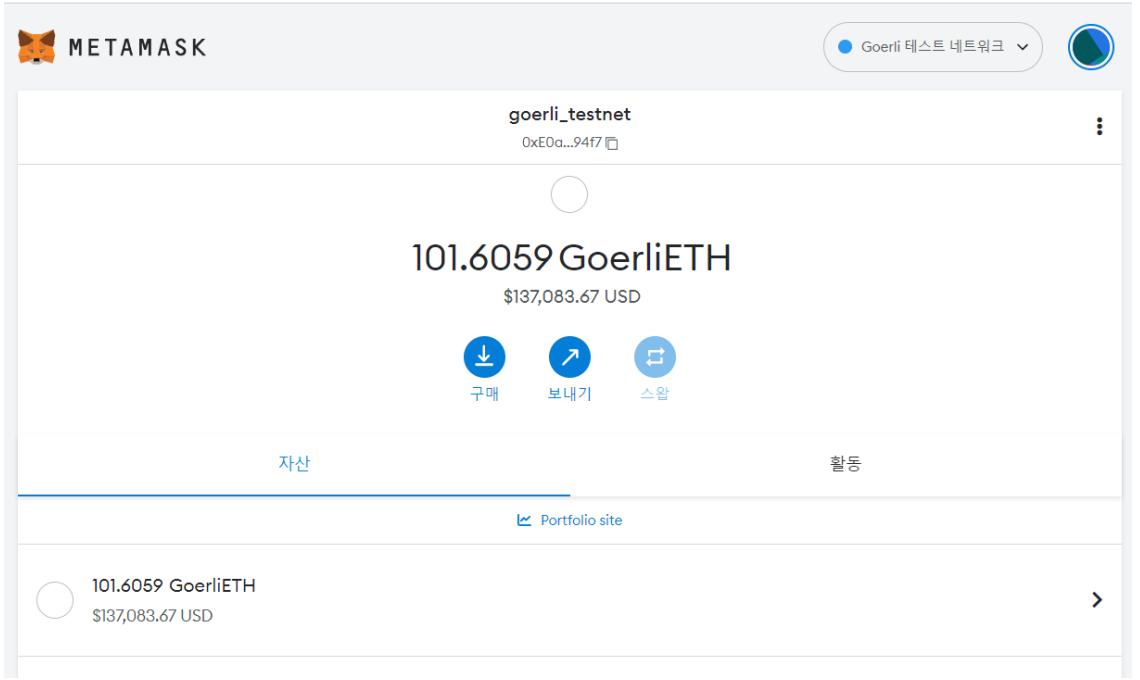


- 지갑은 블록체인이 아니며, 블록체인 네트워크의 계정을 관리 할 수 있도록 도와주는 프로그램
- 하나의 계정에 여러 개의 블록체인 계정을 관리할 수 있음
- 각 계정들은 개인키에 의해서 생성됨

블록체인 지갑

지갑은 왜 필요한가?

```
$ geth --datadir /e/ethereum_privateNetwork/node1 init genesis.json
INFO [03-02|16:20:35.577] Maximum peer count                       ETH=50 LES=0
total=50
INFO [03-02|16:20:35.656] Set global gas cap                       cap=50,000,00
0
INFO [03-02|16:20:35.656] Allocated cache and file handles         database=E:\e
thereum_privateNetwork\node1\geth\chaindata cache=16.00MiB handles=16
INFO [03-02|16:20:35.971] Writing custom genesis block
INFO [03-02|16:20:35.988] Persisted trie from memory database      nodes=7 size=
893.00B time=16.7556ms gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.0
0B
INFO [03-02|16:20:35.991] Successfully wrote genesis state         database=chai
ndata hash=945154..f79f6d
INFO [03-02|16:20:35.991] Allocated cache and file handles         database=E:\e
thereum_privateNetwork\node1\geth\lightchaindata cache=16.00MiB handles=16
INFO [03-02|16:20:36.479] Writing custom genesis block
INFO [03-02|16:20:36.480] Persisted trie from memory database      nodes=7 size=
893.00B time="521.3µs" gcnodes=0 gcsize=0.00B gctime=0s livenodes=1 livesize=0.0
0B
INFO [03-02|16:20:36.482] Successfully wrote genesis state         database=ligh
tchaindata hash=945154..f79f6d
```



블록체인 지갑

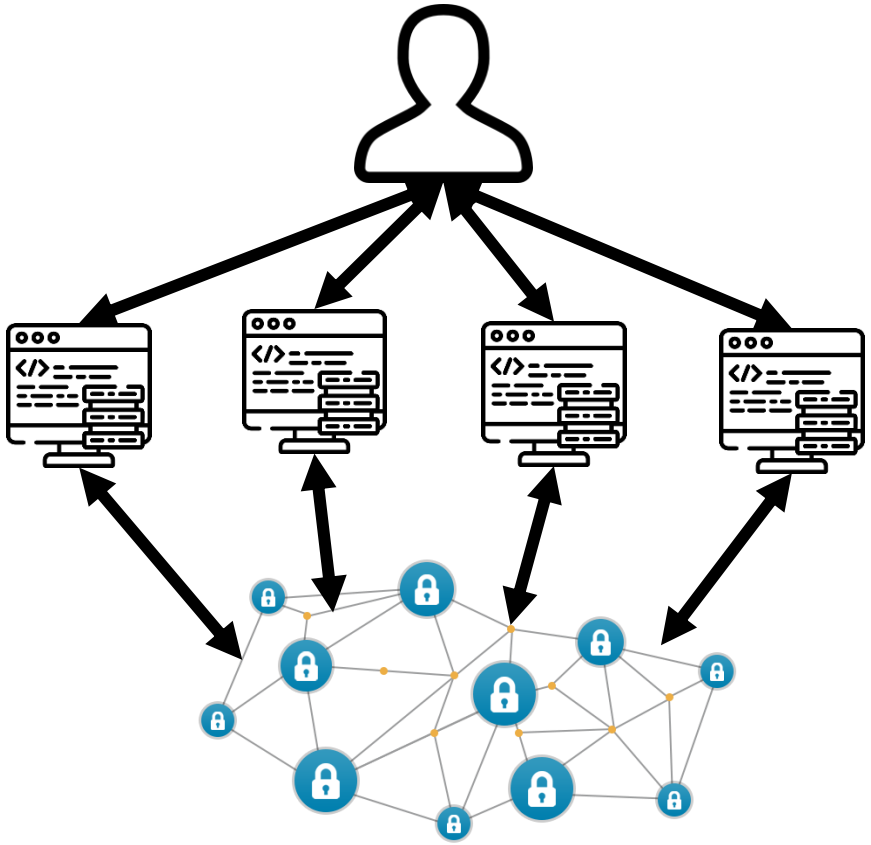
지갑의 중요성

- 개인키를 생성 및 관리를 효율적으로 진행 가능
- 지갑의 보안에 따라서 가상 자산 보호가 가능
  - 암호화폐가 탈취당했다 = 지갑이 해킹에 노출되었다

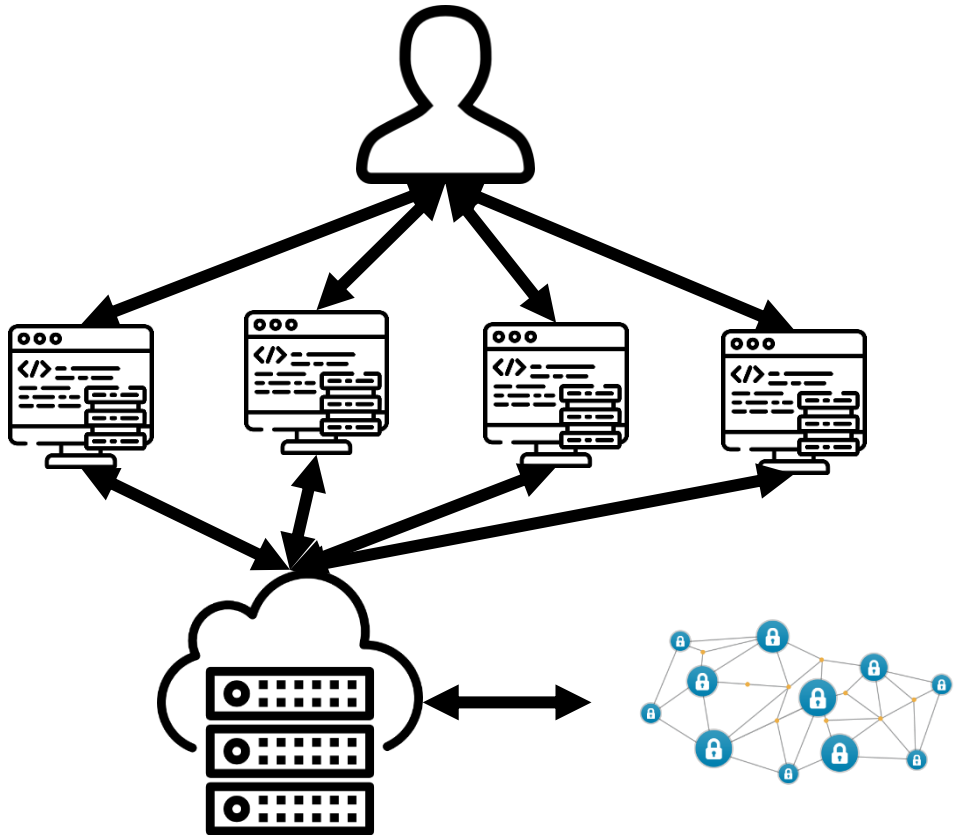
블록체인과 DApp

Decentralized Application
블록체인 기반의 Application

이상적인 DApp



현실적인 DApp



블록체인과 DApp


GamingonPhone
AXIE
INFINITY


Mythical Games
SELECT GUMBALLS
TAKO
160
114534
FRUIT PUNCH GUMBALL
Replace the base color of your Mash-Up with a punchy red flavor during a Mix or a Mash-Up.


Akantor
Round 1
End Turn


Blockchain Gaming World
N.O.O.B.
4415
5800
WATERMELONIE
DETAILS
SKILLS
ACCESSORIES
SEASON
00
ISSUE
2055
3092
LEVEL
10
15
XP
59%
SKILLS CATEGORY
SPEEDSTER
ARTIST: MARK JONES
Open Beta Edition! Watermelonie may look sweet, but this Blanko is all spit and vinegar. To call her hardheaded would be an understatement. If you somehow manage to break that impenetrable rind, rest assured, Watermelonie will bite back.

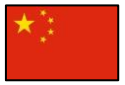
CBDC

중앙은행이 발행하는 가상화폐

저개발 국가

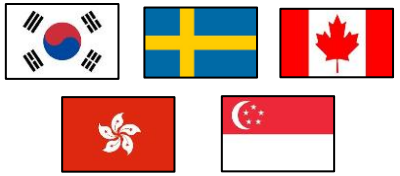
- Unbanked 해소
- 소매시장 내 자국 통화 영향력 확대

금융취약 강대국



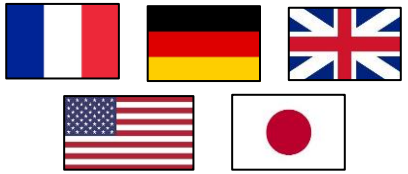
- 금융제도 혁신
- Payment 혁신
- 디지털 경제 활성화

금융선진 중소국



- FinTech 진흥
- 디지털 경제 중심 경제 성장 전략

금융선진 강대국



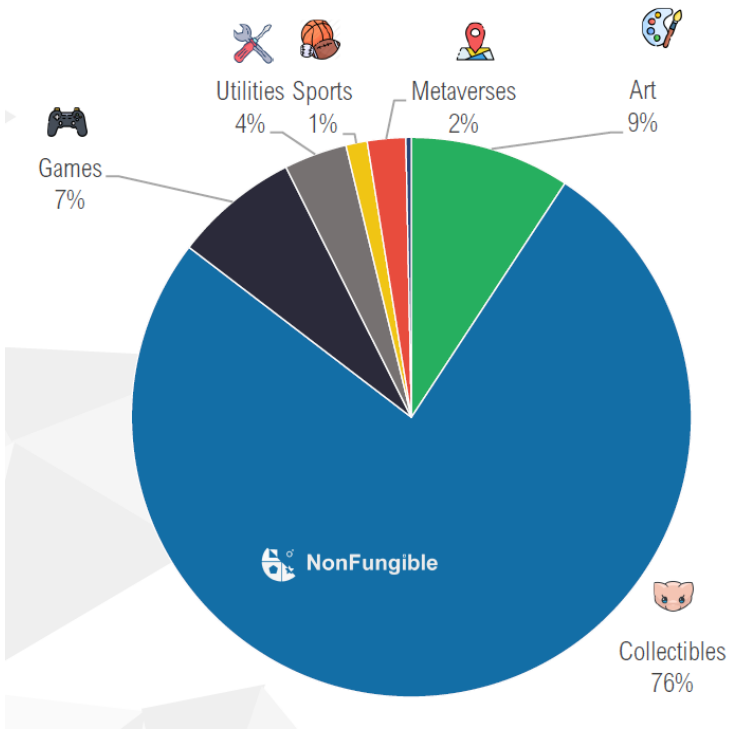
- 자국 통화 영향력 유지
- 디지털 산업의 제도적 기반 선도
- 저비용 통화/재정 정책 수단 보급

디지털 자산의 소유권을 증명하는 NFT

- 기존의 현물 거래는 거래 기록을 확인 가능
- 기존의 디지털 자산은 손쉬운 파일 복사로 인해 소유주 증명 불가능
- NFT는 블록체인을 통해 거래 내역을 증명할 수 있으므로 소유주 증명 가능
- 기존에는 거래가 불가능했던 상품에 대한 새로운 거래 시장 형성

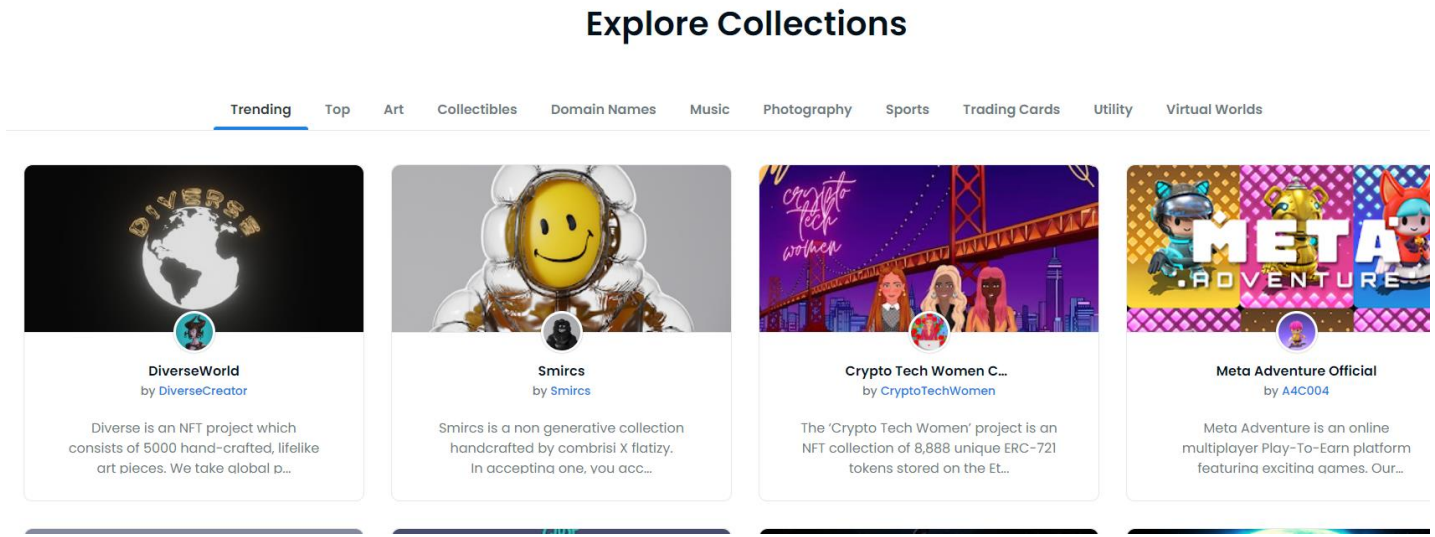
NFT와 블록체인

NFT 현황



Non-fungible Tokens Quarterly Report Q3-2021

Opensea



NFT의 활용

1. 디지털 예술품 거래 시장

CryptoPunk #7523

JA MORANT DUNK Legendary #42/49

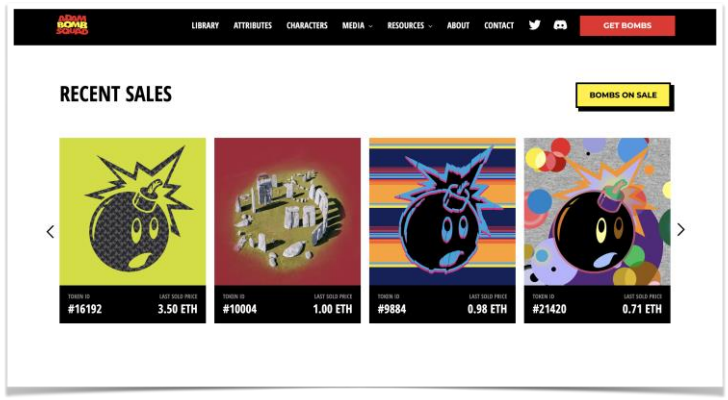
- 디지털 예술품 거래가 이루어지는 시장

2. 커뮤니티 멤버십

- NFT 작품 시리즈를 가지고 있는 사람들끼리 모임 생성

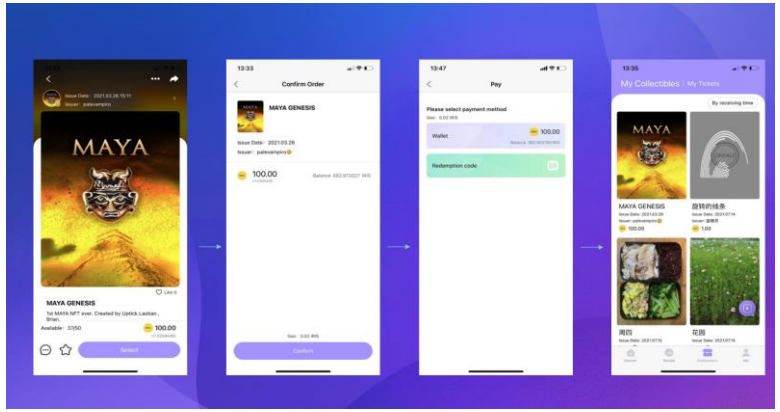
NFT의 활용

3. 브랜드 세계관 확장



- 유명 브랜드가 자신들의 팬덤 및 세계관 확장을 위해 NFT 시리즈를 발행

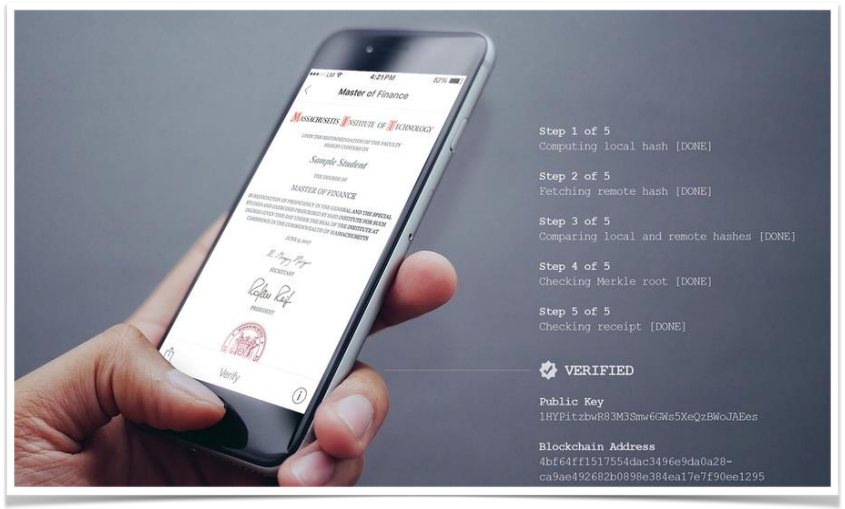
4. 실생활 응용



- 레스토랑 예약권, 멤버십 카드
- 공연 티켓을 NFT로 판매해 굿즈로서의 소장 욕구 자극

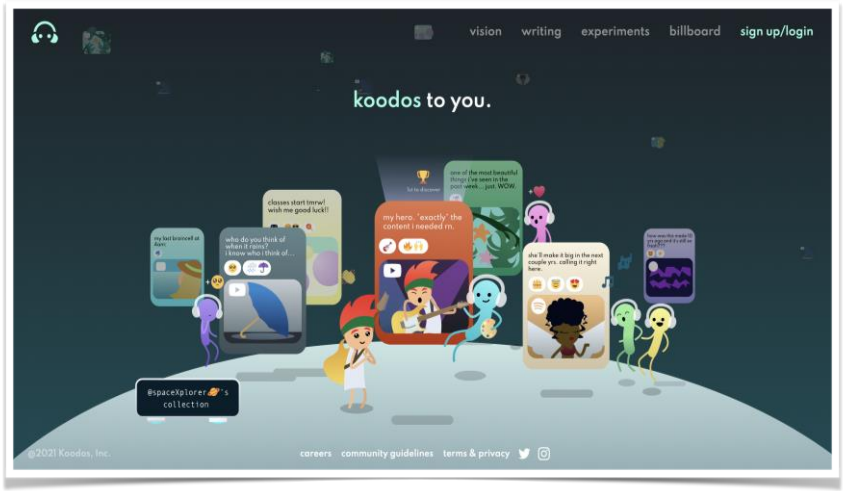
NFT의 활용

5. 양도 불가 NFT



- MIT의 새로운 졸업장 배포

6. NFT 발행 플랫폼

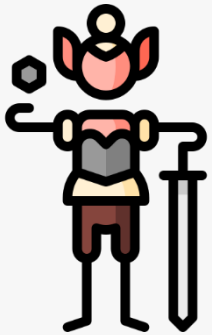


- NFT를 쉽게 발행 및 공유 가능한 서비스 제공

기존의 가상 세계

현실과 연관성이 없는 하나의 세계

가상 세계의 나



군주

암살자

부자

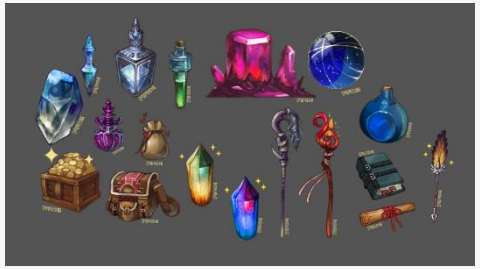
현실 세계의 나

학생

회사원

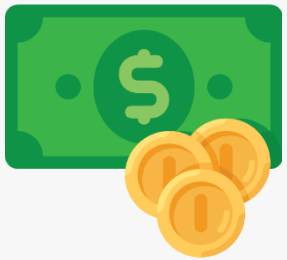
오늘날의 가상 세계 (Metaverse)

가상 세계의 자산



상호연결

현실 자산



메타버스와 블록체인

아바타 드라마 작가와 PD

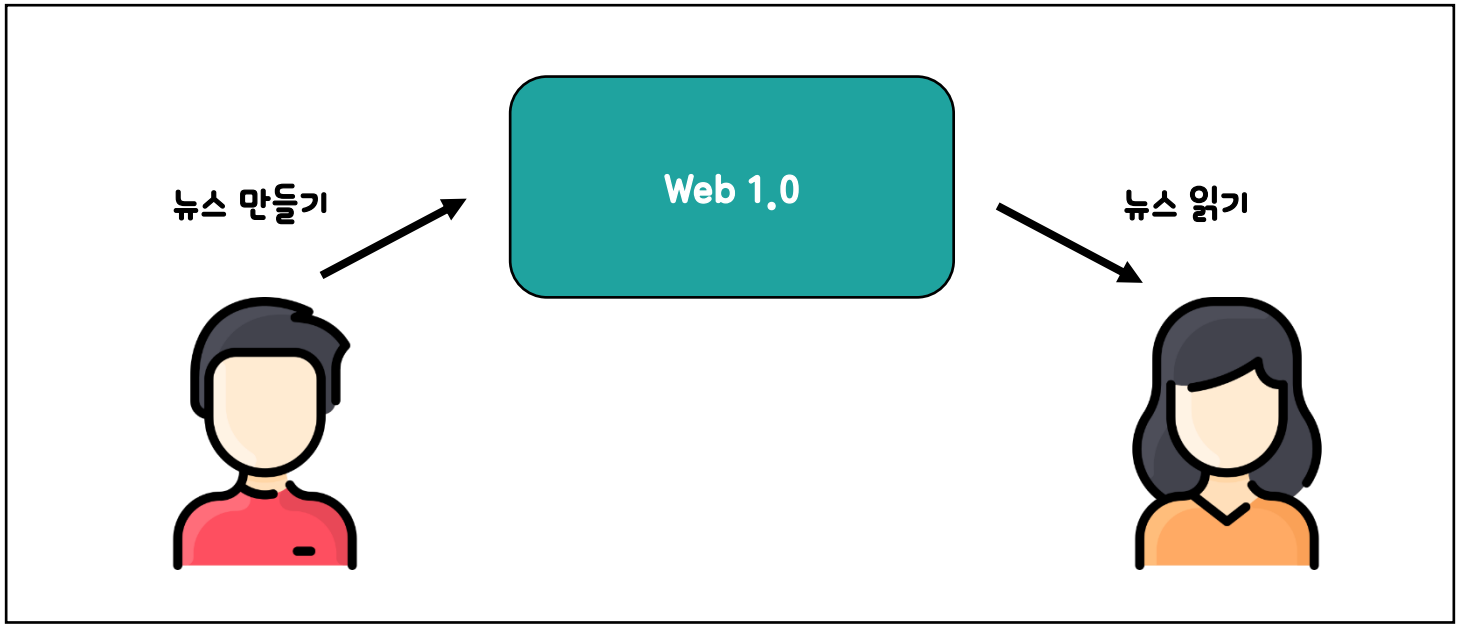
아이템 디자이너

월드 빌더

ROBLOX 개발자

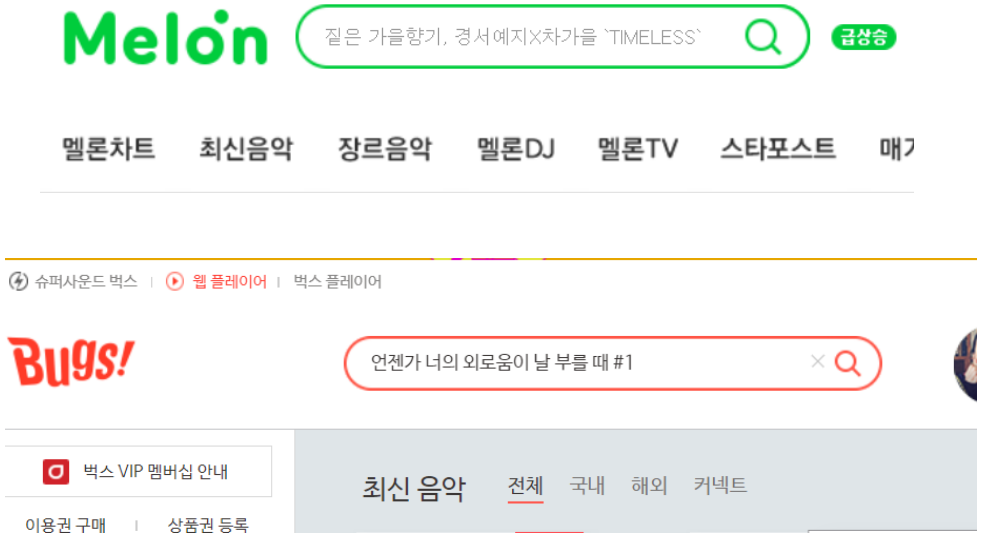
Web 1.0의 한계

- HTML, URL 등의 단순 정보 제공 수단으로 사용되었던 고전적인 웹의 형태
- 이용자는 '뉴스 만들기'와 같은 'Write' 기능을 사용할 수 없고, 'Read' 기능만 사용할 수 있음
- 단방향적 소통방식



Web 2.0의 한계 - 데이터의 독점화(중앙화)

- 중앙화된 데이터를 제어하고 사용하는 서비스를 제공하는 거대 플랫폼
- Web 2.0은 거대 플랫폼의 데이터 중앙화를 가속



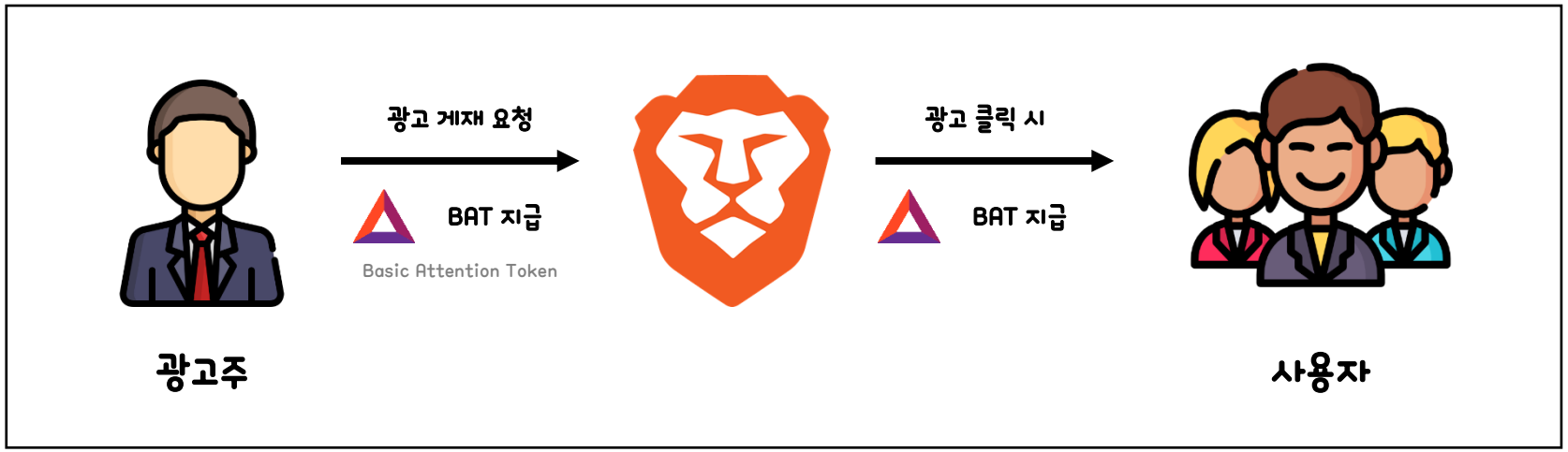
- 데이터 사용 독점 및 단절
- 거대 빅테크 독점에 의한 생태계 지속 가능성에 대한 우려

Web3

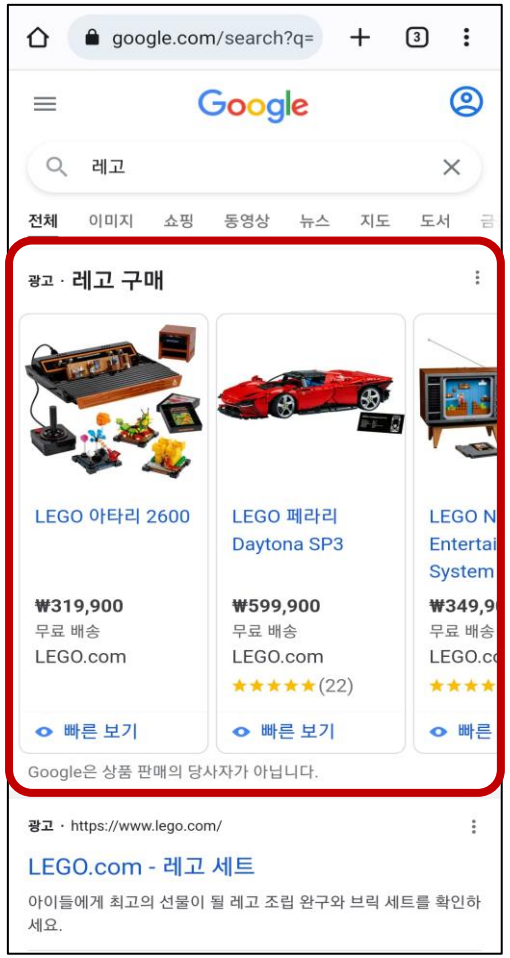
- 유저가 읽기, 쓰기, 소유 가능
- 소유를 위한 암호화폐 사용
- 주식회사의 주식과 비슷한 개념이나, 투명하고 알고리즘에 의해 공정하게 배분됨
- 사용자들이 자신의 콘텐츠의 경제적 가치를 누릴 수 있고 플랫폼 운영에도 참여가능

Brave Browser

- 광고 차단
- 웹사이트 트래커 차단
- 광고 허용 설정을 통해 이용자는 광고를 보고,
  클릭할 경우 BAT 토큰을 받을 수 있음

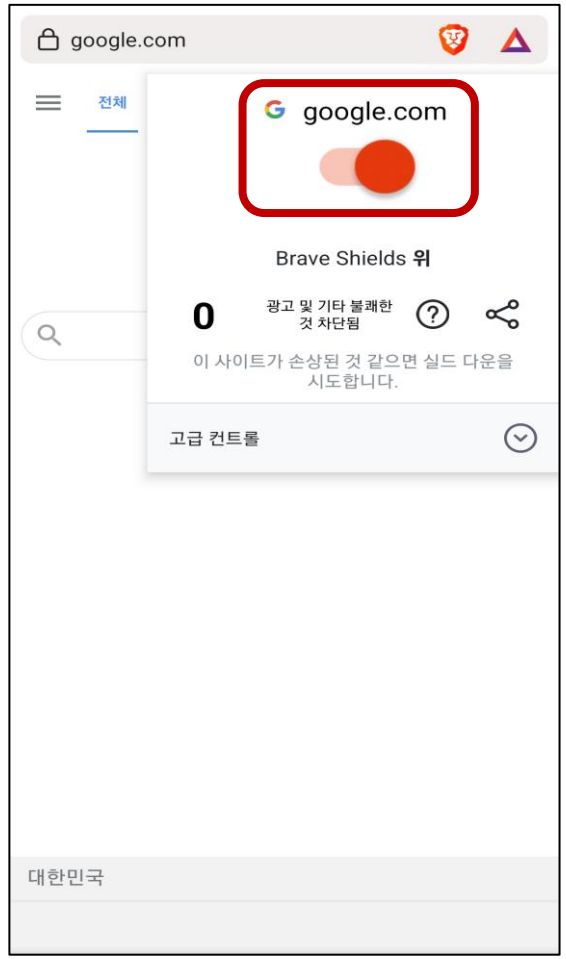


WEB 3.0과 블록체인



Chrome으로 '레고' 검색 시 상단에 뜨는 광고

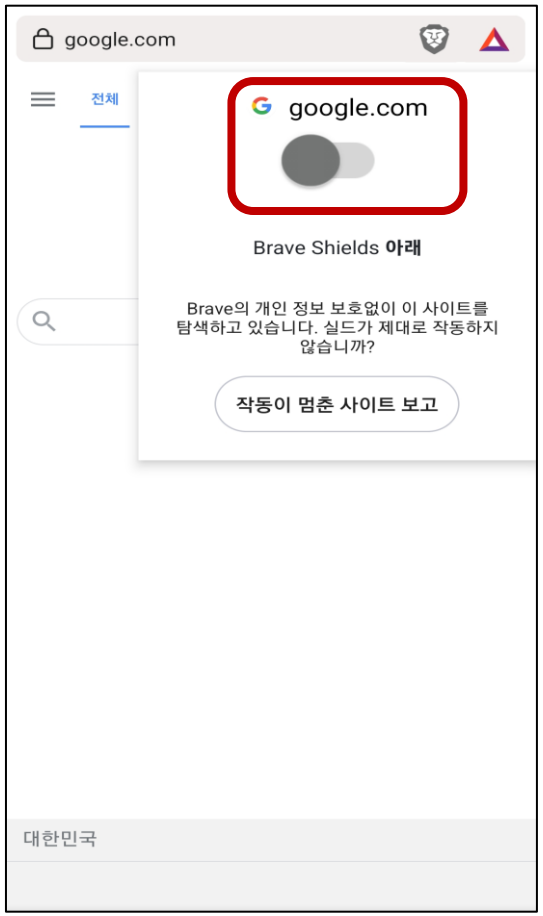
Brave로 광고를 차단하고
'레고'를 검색한 결과



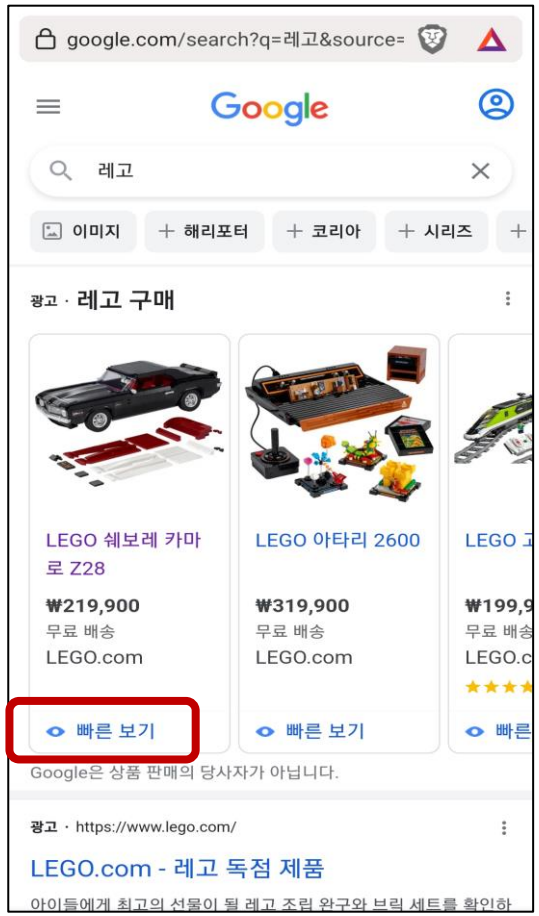
광고 차단 설정

광고가 차단됨

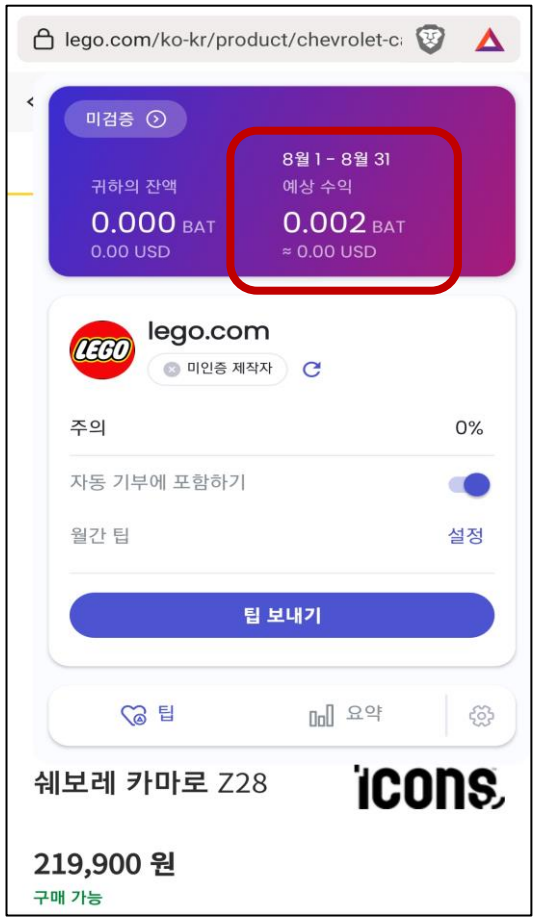
WEB 3.0과 블록체인



광고 허용

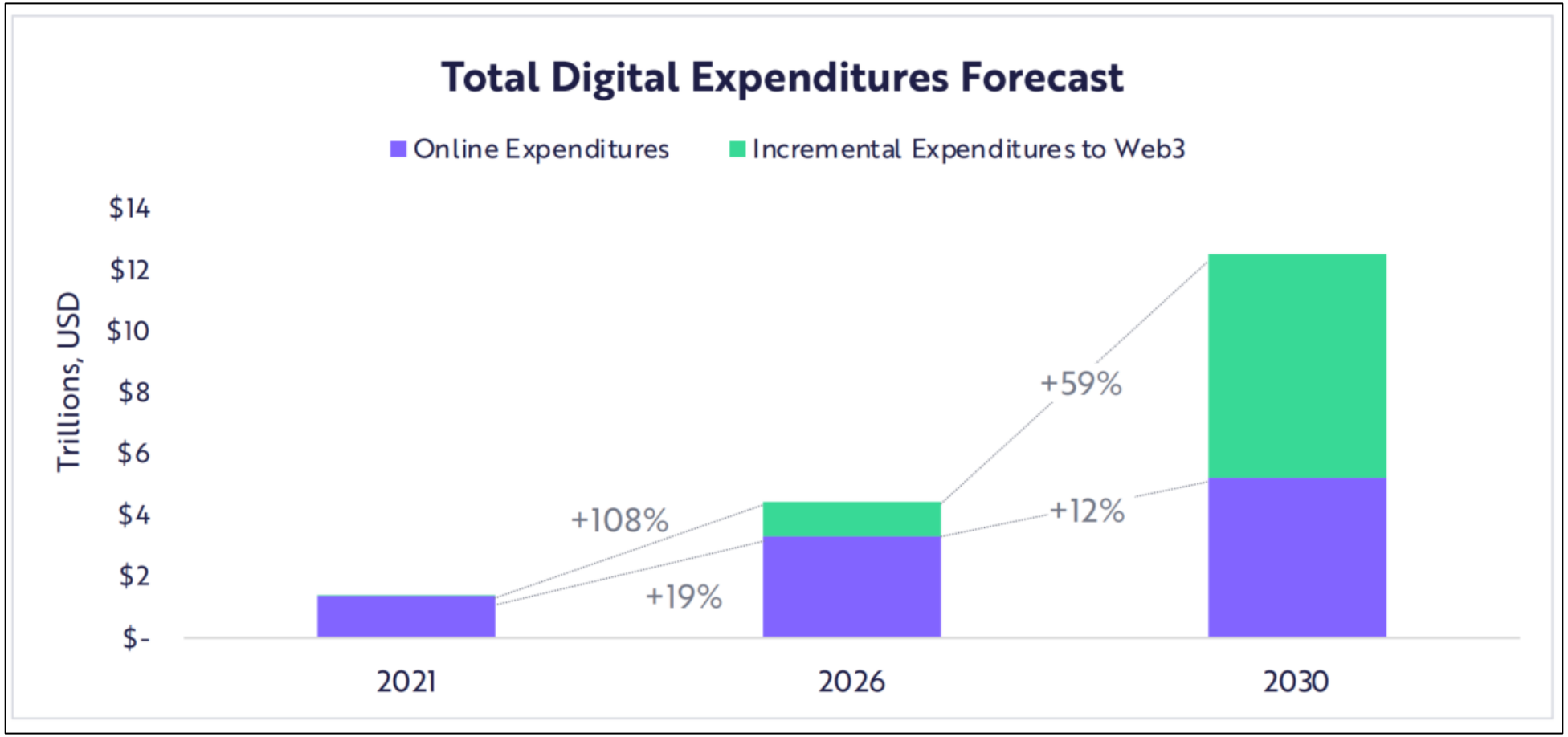


광고 클릭



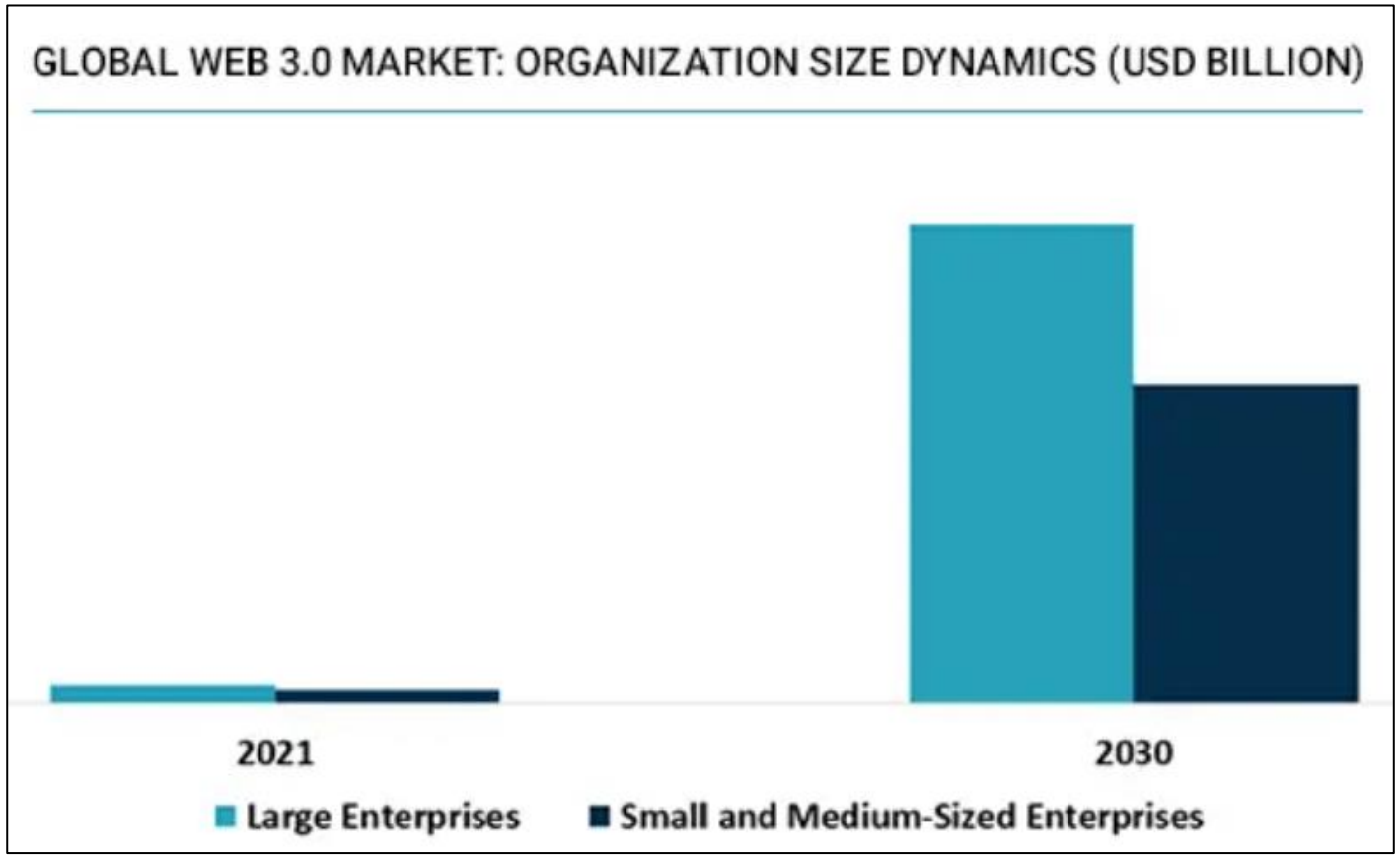
BAT 수익 발생

Web3로 인한 연간 온라인 지출 규모는 2030년에 연간 12.5조 USD에
달할 수 있다는 전망 제시 (미국 ARK Invest Big Ideas 2022)



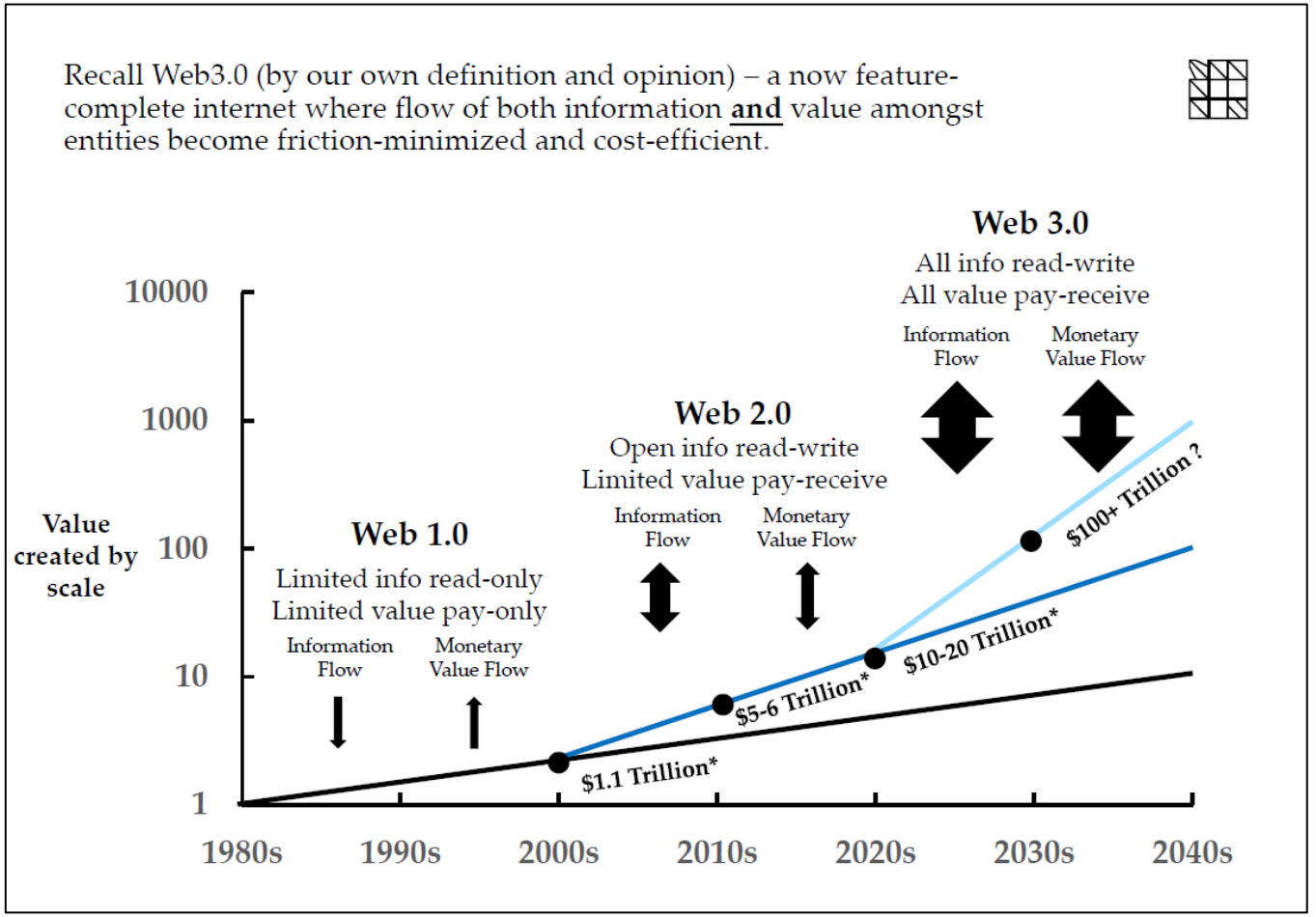
Source: ARK Investment Management LLC, 2021

2021년 $3.2 billion - 2030년 $81.5 billion (CAGR 43.7%)



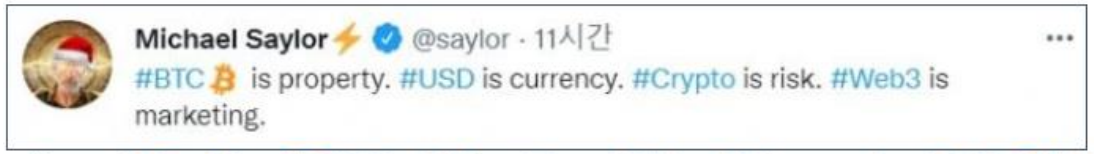
Source: EMERGEN Research 2021

인터넷 기업들의 시가 총액은 2030년 100조 USD를 상회할 것으로 예측 (Capital IQ)

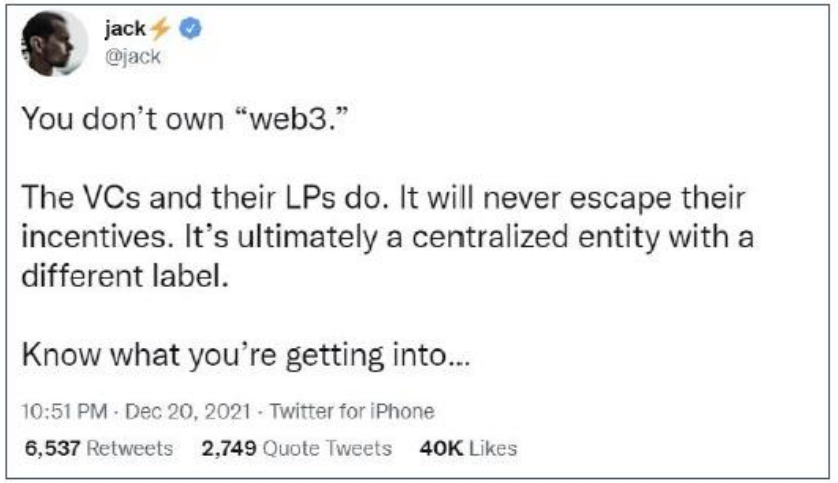


출처: Capital IQ, Public Internet Companies Market Cap (인터넷 기업 예상 시가 총액)

WEB 3.0과 블록체인



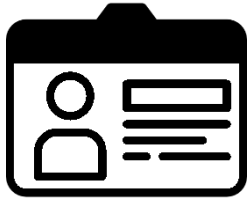
비트코인은 자산, 미국달러는 화폐, 크립토가 리스크라면 Web3는 마케팅 용어이다.



마치며

코인

스마트 컨트랙트



분산 신원 인증

탈 중앙화 금융

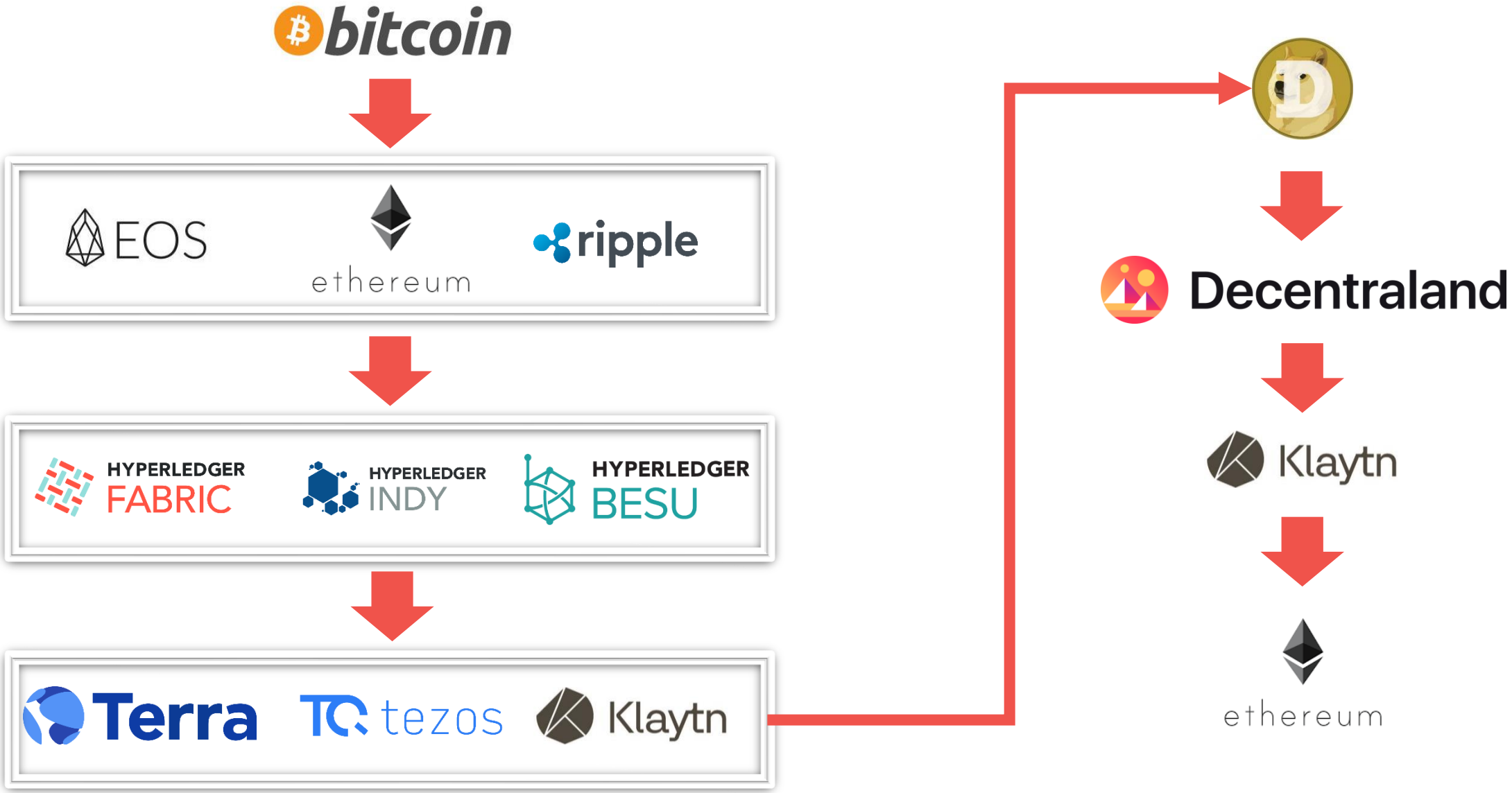
Metaverse

Web3

Non-fungible Token

Play to Earn

아치여


bitcoin
EOS
ethereum
ripple
HYPERLEDGER FABRIC
HYPERLEDGER INDY
HYPERLEDGER BESU
Terra
tezos
Klaytn
Decentraland
Klaytn
ethereum

Q & A