

# 블록체인에 발가락 담가보기

블록체인을 모르는 사람들을 위한 시간

블록체인 왜 배워야 하나요?



# 블록체인 왜 배워야 하나요?

1. 잘 돌아가고 있는 기존 인프라를 바꿀 필요는 없다
2. 신흥국을 움직일 블록체인
3. 부패한 중개자를 배제한, 신속하고 투명한 원조
4. 블록체인이 바꾸는 사회, 탈중앙화와 검열저항성
5. 초연결사회, 4 차 산업혁명의 핵심이 될 블록체인
6. 블록체인이 해결해야 할 과제: 기술은 번영을 보장해주지 않는다

요약 출처: [https://choonsik.blogspot.com/2018/05/blog-post\\_15.html?sref=fb](https://choonsik.blogspot.com/2018/05/blog-post_15.html?sref=fb) (요약 리뷰 블로그)  
원본 출처: <https://bit.ly/2Ksi9ll> (한화투자증권 김열매 연구원님 리포트)

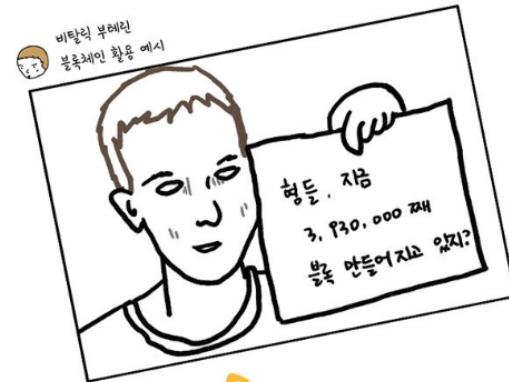
# WHO AM I

- ❑ Vassar College: Media Studies
- ❑ Fortune Magazine: Website Production
- ❑ 판교 모회사 BlockChain
- ❑ 연극 → 미디어 → 미디어/아트 + 테크
- ❑ 딥러닝 공부: 모두의 연구소 Deep Learning College 영상처리
- ❑ 블록체인 업무
- ❑ 개발

# 이런 분들은 회식 때 다시 만나요...

- 이미 유튜브로 블록체인 관련 강의들을 2-3개 이상 들어봤다.
- 이더리움, 비트코인 관련 기술 책을 읽어봤다.
- 일주일에 한 번 이상 “블록체인” 이야기를 한다.
- 블록체인 밋업이나 스터디를 가보았고 이해가 70% 이상 되었다.

# 오늘의 목표 중의 하나...

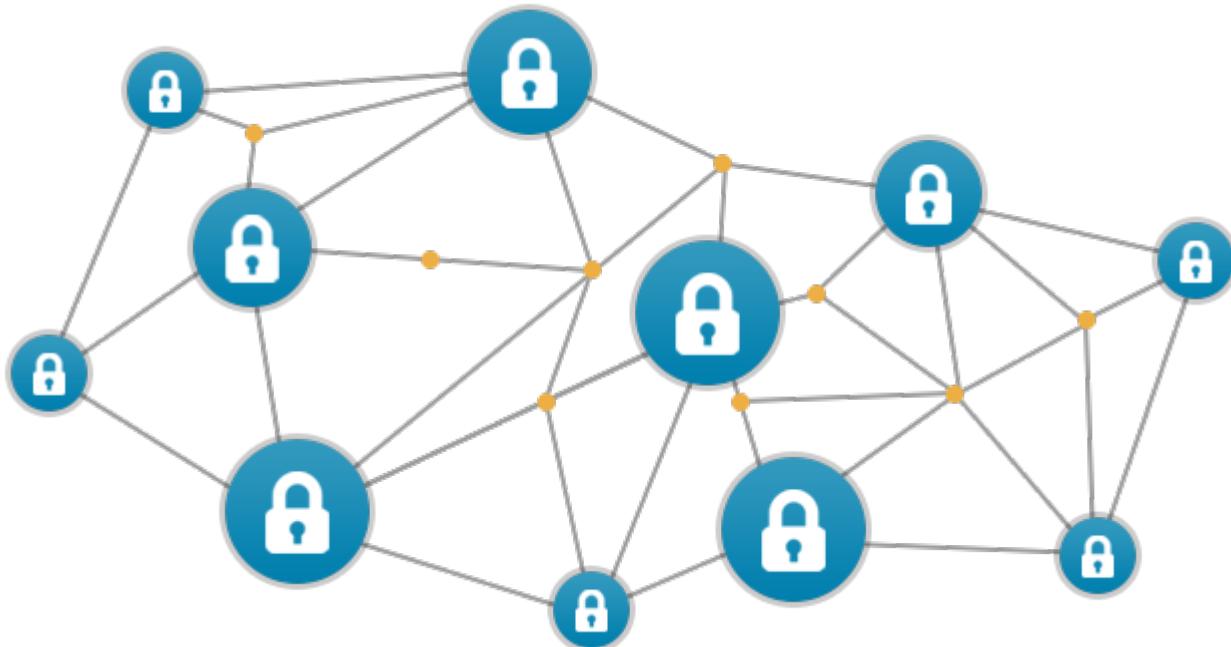


(부레린 사망설이 떠돌자 부레린이 당시 이더리움 블록에서 생성되는 블록 숫자를 종이에 적어 트위터에 올렸고, 한 신문에서 이를 PoL, Proof of Life이라 했다.

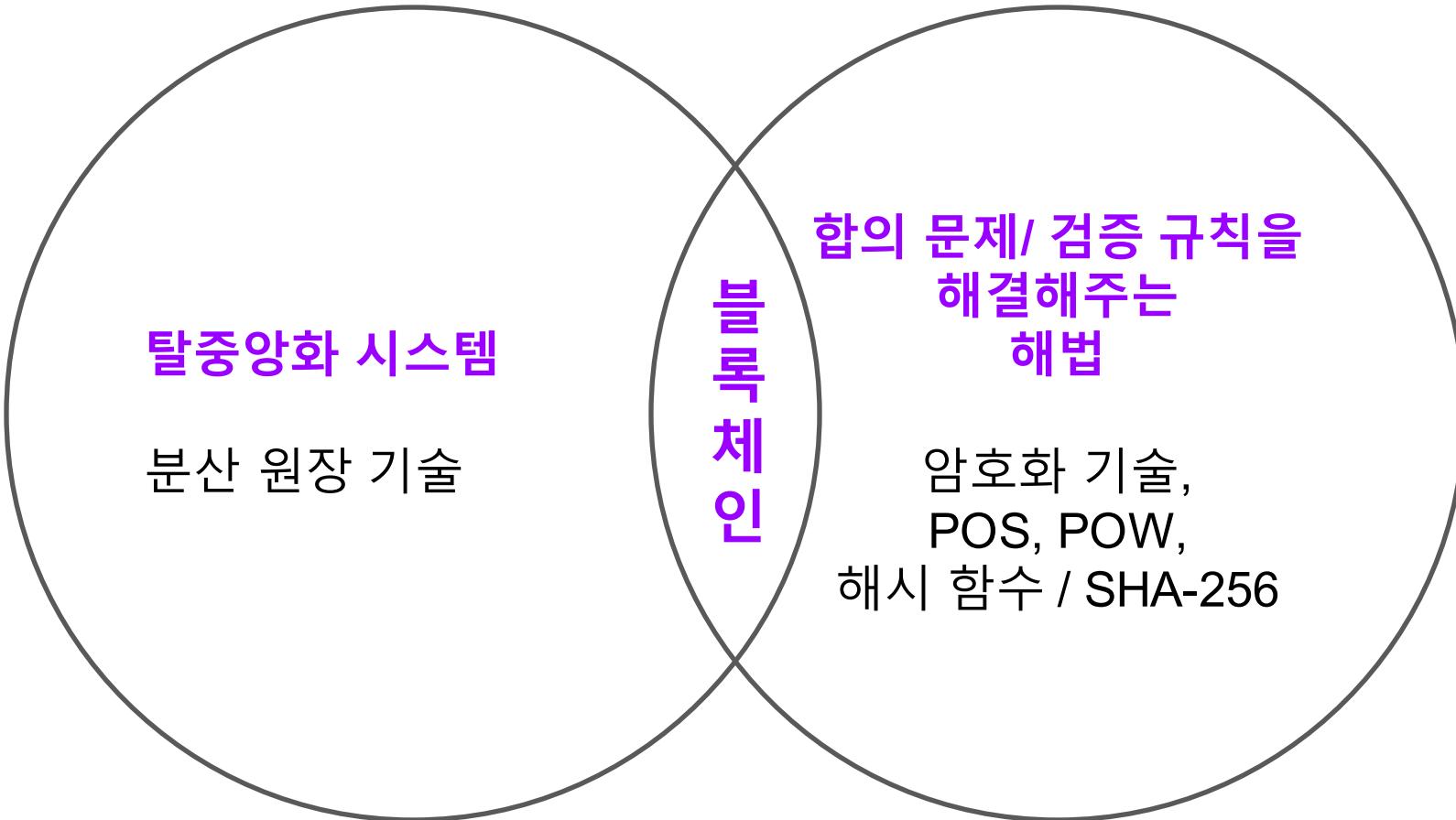


뭐야 그게 ..

웹툰 이미지 출처:  
<https://steemkr.com/webtoon/@leesol/webtoon-gopax-x-leesol-5-feat-pow-and-pos> ,  
<https://imgur.com/4Byv1n2>



이미지 출처:  
[https://www.draglet.com/blockchain-  
services/private-or-public-blockchain/](https://www.draglet.com/blockchain-services/private-or-public-blockchain/)



암호 화폐



탈중앙화  
시스템

합의 문제,  
검증 규칙

POW 채택

게임을  
시작하지

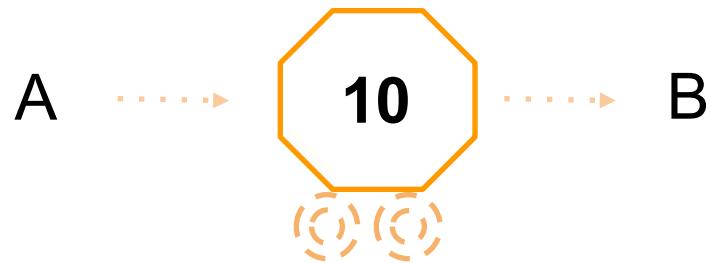
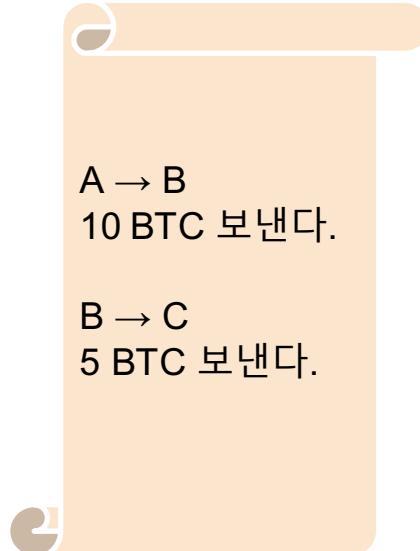
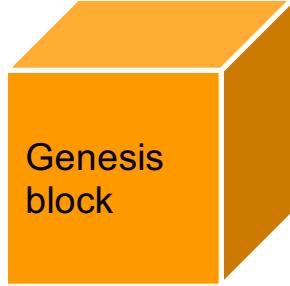


# 비트코인 시뮬레이션

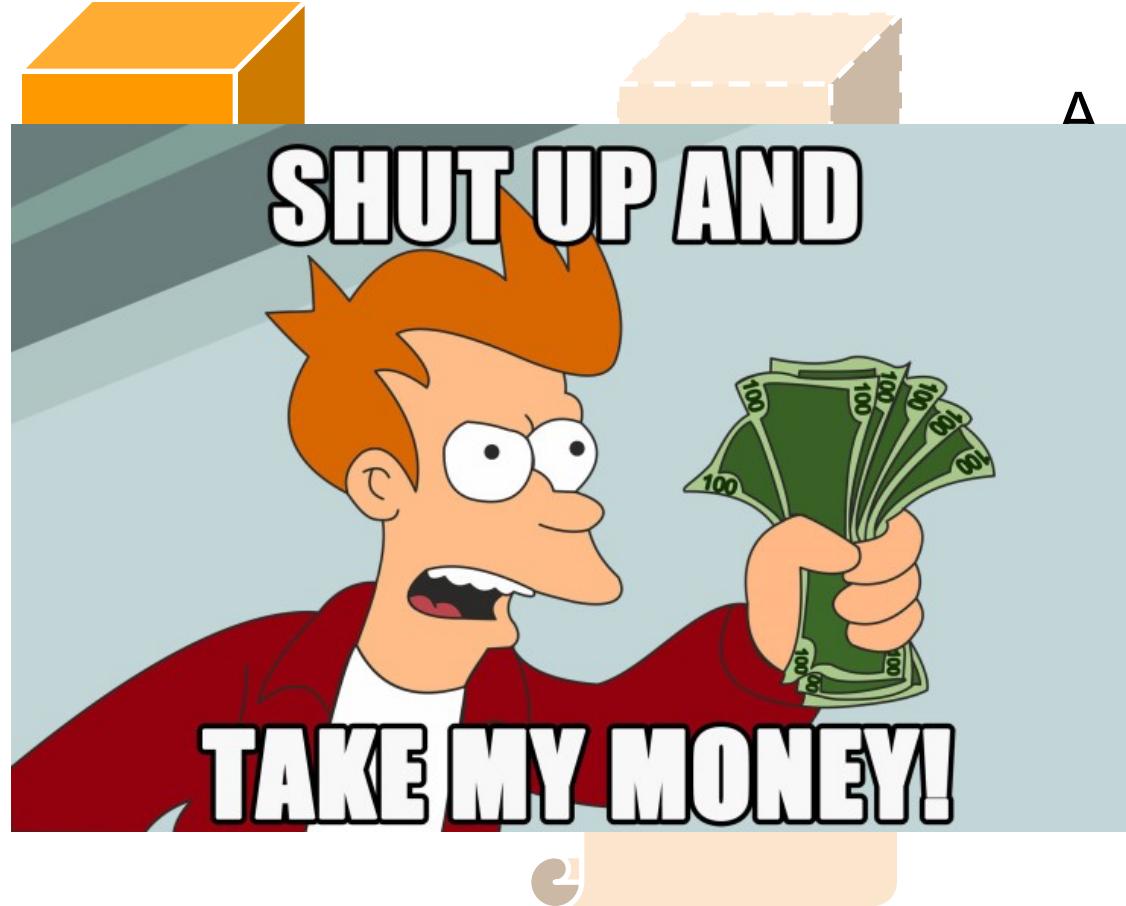
- A, B, C, D, E. 각자가 노드입니다. 노드 = 컴퓨터 = 개인 = 참여자 = 너 = 나
- 각자 노트를 한 장씩 가집니다. 트랜잭션을 기록할 곳입니다. (distributed ledger)
- 계산기/뇌 = 채굴하는 컴퓨팅 파워

비트코인처럼 PoW Proof of Work

를 사용하는 시스템에만 쓰입니다.



10BTC를 보내려는데, 보상 줄테니까 (수수료),  
내 돈 좀 보내줄 사람?

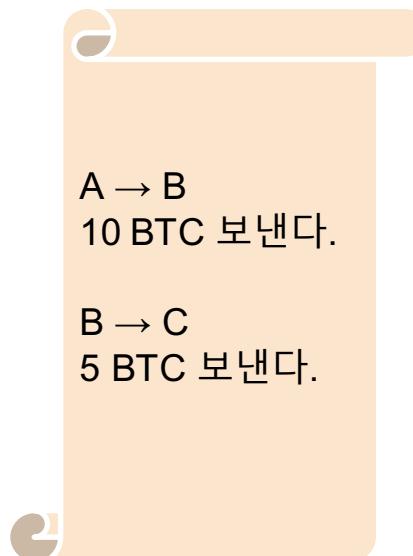
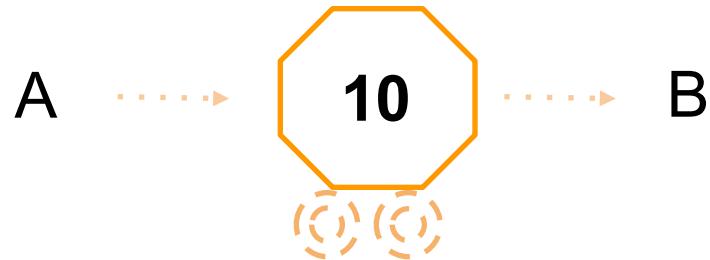
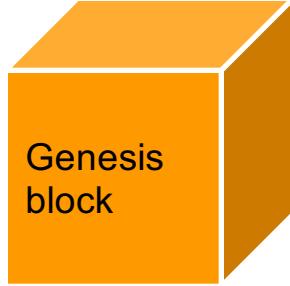


△

10

B

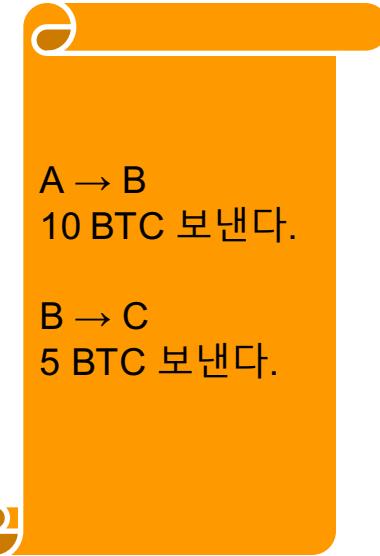
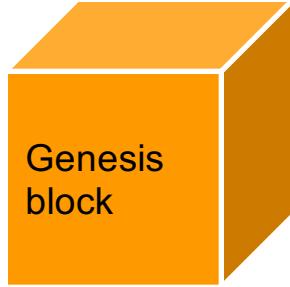
내 돈 좀 보내줄 사람?



내 돈 좀 보내줄 사람?

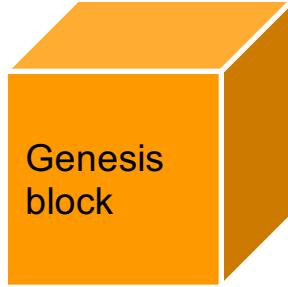
$X + 3 = 5$   
X를 구하시오.  
제일 먼저 해를 찾는 사람이  
수수료를 GET 합니다.

이렇게 여러 트랜잭션들이 발생합니다.  
그 트랜잭션들이 발생하는 동안 누군가  
는 해를 구하고 있습니다.



누군가가 해를 구했다!

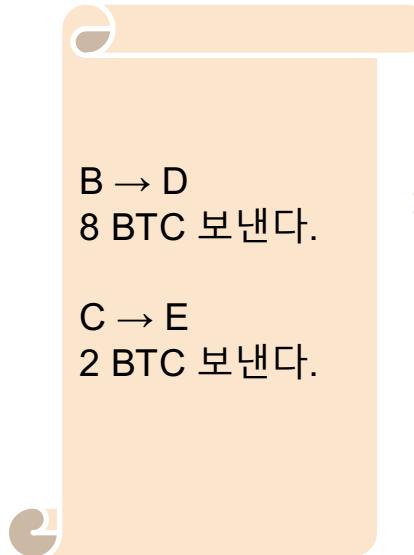
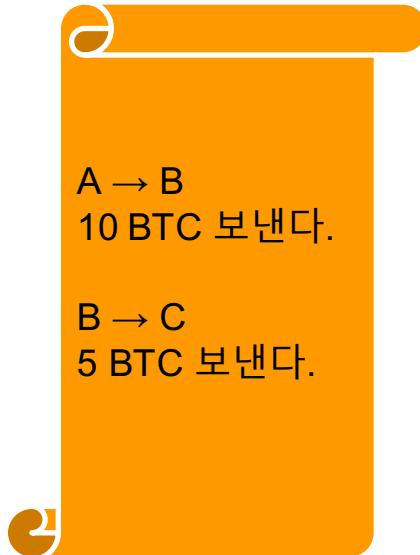
블록이 생성되고  
그 블록 안에 트랜잭션 기록들  
이 저장되어 함께  
유효화된다.



$$x^2 - 3x - 4 = 0$$

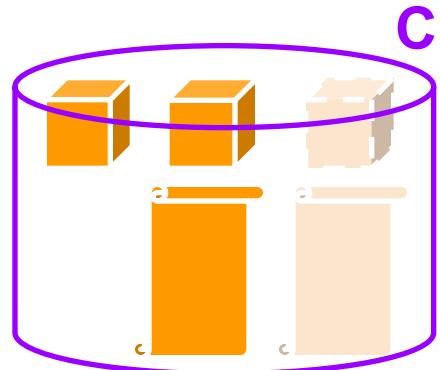
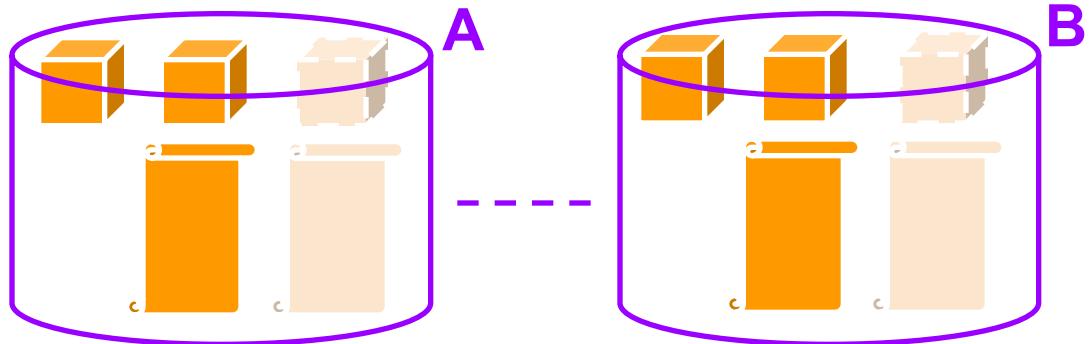
$$\cos(x) = 1/2$$

블록마다  
점점 어려  
워지는  
문제



Find the eigenvalues and eigenvectors of the matrix

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}.$$



탈중앙화  
합의

$$x^2 - 3x - 4 = 0$$

$$\cos(x) = 1/2$$

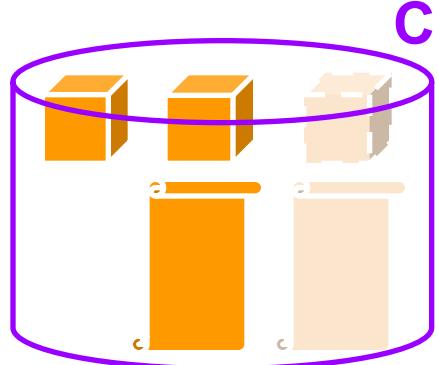
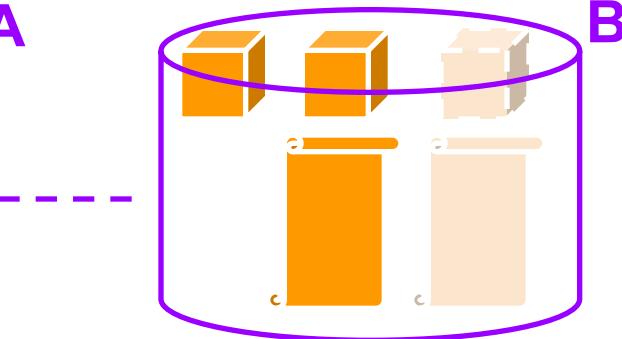
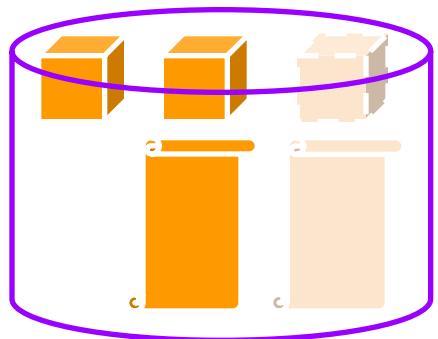
Find the eigenvalues and eigenvectors of the matrix

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}.$$

난이도가 점점 증가하면서  
컴퓨팅파워들도 강해짐.

블록 생성 시간을 일정하게 유지.

‘해’가 풀리는 시간과  
들어가는 작업량(WORK)을  
고려해서 난이도를  
계속 조절하며 상향시킨다.



탈중앙화  
합의

~~$x^2 - 3x - 4 = 0$~~

~~$\cos(x) = 1/2$~~

Find the eigenvalues and eigenvectors of the matrix

$$A = \begin{pmatrix} 1 & -3 & 3 \\ 3 & -5 & 3 \\ 6 & -6 & 4 \end{pmatrix}.$$

실제로 블록체인에서 작업증명으로  
구하는 ‘해’는 ‘난스’이다.

퍼즐의 정답:  
해시 퍼즐의  
‘난스’

# 해시 함수 | SHA 256

1	2	3	4	5	6	7	8	9	10	11	12	13	14	15	16	17	18	19
ㄱ	ㄴ	ㄷ	ㄹ	ㅁ	ㅂ	ㅅ	ㅇ	ㅈ	ㅏ	ㅓ	ㅡ	ㅣ	ㅎ	ㄲ	ㄸ	ㅃ	ㅆ	ㅉ
20	21	22	23	24	25	26	27	28	29									
ㅏ	ㅑ	ㅓ	ㅕ	ㅗ	ㅛ	ㅜ	ㅘ	ㅡ	ㅣ									
30	31	32	33	34	35	36	37	38	39	40	41	42	43	44				
0	1	2	3	4	5	6	7	8	9	,	.	!	?					

비트코인 = ㅂ(6)+ㅣ(29)+ㅓ(12)+ㅡ(28)+ㅓ(11)+ㅗ(24)+ㅇ(8)+ㅣ(29)+ㄴ(2)= 149

입력

출력

그림 4-1 간단한 해시 함수

블록체인에서 쓰는  
SHA-256 해시 함수

**SHA-256: 불규칙성, 작  
은 차이에도 완전히 다른  
결과 값, 예측 가능성 제  
로**

# 해시 함수 | SHA - 256 | 난스

비트코인 난스8	:	1e193280c417d1542f51d2d24
비트코인 난스9	:	14ea22642f6580206d28aa43d1cbab194f
비트코인 난스10	:	89c5348e84e1715a577c6de497001d2d24
비트코인 난스11	:	d5c236680444e552d4f528f0726abb4710
비트코인 난스12	:	159576c096c767e01335e883750e007ef9
비트코인 난스13	:	2e2e0ce0fccaa93bfcc7b013b8f7e385196
비트코인 난스14	:	0910c32ba6945e361de5a96ba1d5ba1df5
비트코인 난스15	:	83261c8c16d89adc4ee5a91bbf9dd93285

예를 들어, 지금 주어진 목표값이 009acbd.....이  
라면 난스 58이 더 작으니까  
내가 찾은 해가 될 것  
난스 14 결과값 > 009acbd... > 난스58 결과값

비트코인 난스57	:	c0720ce2252125514b92c1f88427781b74
비트코인 난스58	:	006ac0f2f56172bdb073a3433852d61cb6
비트코인 난스59	:	913ad5fff23c9b48b977da3b9694df301c
비트코인 난스60	:	c9346875af783f539d385428f5436af3e0

트랜잭션  
id



난스  
(1, 2, 3.....)

SHA 256  
해시 함수

목표보다 작은  
어떤 결과값

이미지 출처:

비트코인과 블록체인: 탐욕이 삼켜버린 기술 (이병욱 저)

4장 비트코인시스템상세설명

표 4-3 숫자를 증가시킬 때 해시 값 맨 앞에 연속된 0이 나타나는 개수

연속된 0의 개수	뒤에 붙인 숫자	해시 값
1	14	0x0910c32ba6945e361de5a96ba1d5ba1df5d0fc16e5a44cec0267c2b82ae6175b
2	58	0x006acd0f2f56172bdb073a3433852d61cb6bd51388325c1ff275a8462e14d1e69
3	156	0x000410491390eb3e19c13ffbbfed063828c2de465de3e13288477ae27b19ed71
4	70,999	0x0000b285181368d4bbf90ae18c4f25a4c877ab254ddfd8607193aa2f24ec537f
5	1,739,385	0x00000a3d8be4417182d10c463578fa1efd8fd06da3dd7188ebb8fed9e472148d

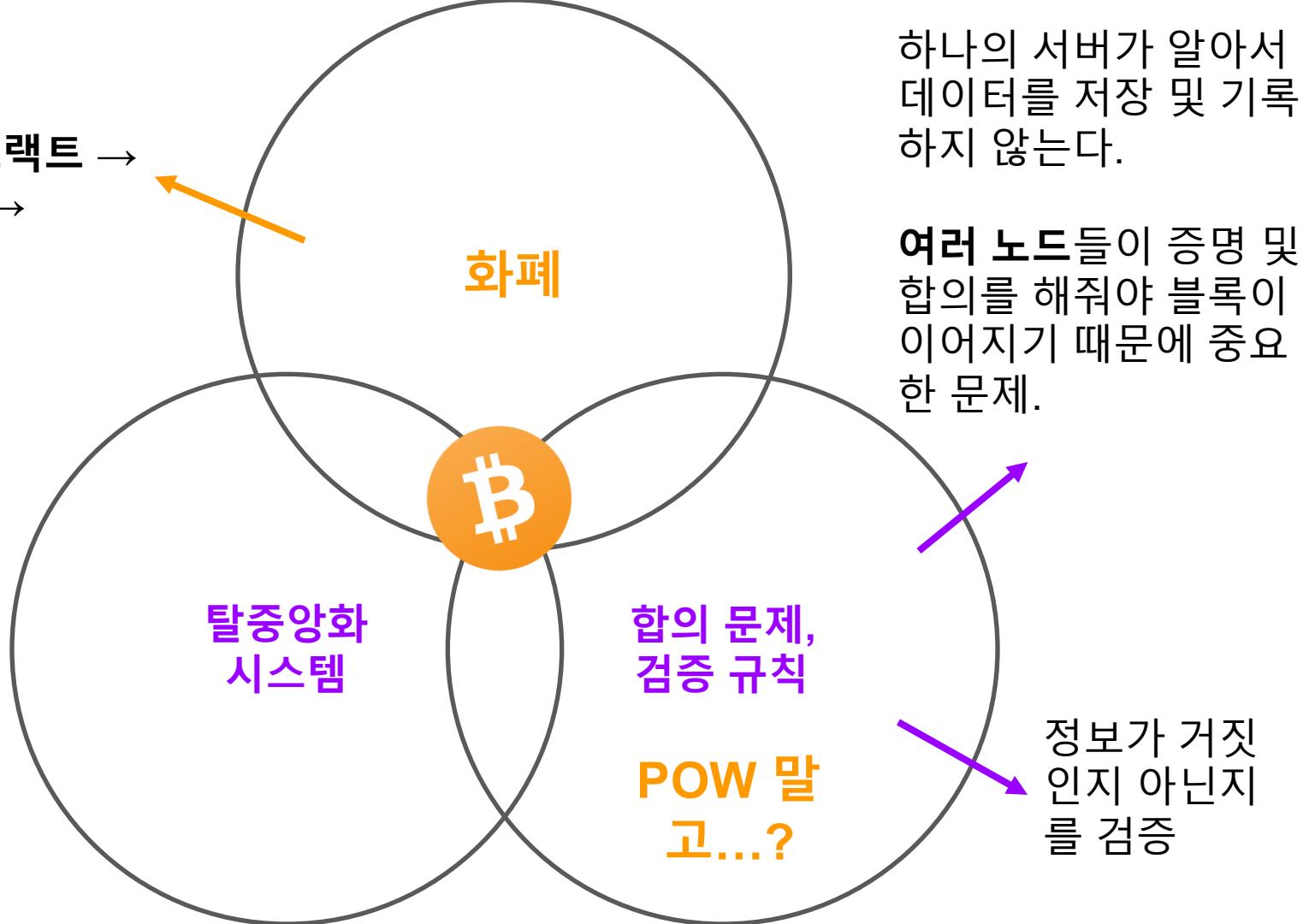
“ 해시 퍼즐이란 숫자를 바꿔가며 SHA-256 해시 값을 만든 후 그 값이 목표 값보다 작아질 때 까지 되풀이하다 목표 값보다 작아지는 순간 찾은 그 값이 바로 난스”

-p.158 비트코인과 블록체인

이미지 출처:

비트코인과 블록체인: 탐욕이 삼켜버린 기술 (이병욱 저)  
4장 비트코인시스템상세설명

화폐 →  
스마트 컨트랙트 →  
앱, 플랫폼 →  
...



**비트코인**

**이더리움**

**스팀잇**

**POW**

**POS**

**DPOS**

**가치거래**

**스마트 컨트  
랙트**

**화폐 거래 위  
주**

**앱을 올리는  
플랫폼**

**소셜미디어  
플랫폼**

**콘텐츠 보상**

400



# CAN THIS 22-YEAR-OLD CODER OUT-BITCOIN BITCOIN?

이미지 출처:

<http://fortune.com/ethereum-blockchain-vitalik-buterin/>

# 이더리움 - Vitalik Buterin

- 러시아 출생, 엑셀과 게임 덕후
- World of Warcraft 하는데 최애 기능을 관리자가 마음대로 빼버림
- 분노의 블록체인 공부
- 공부하면서 쓰기 시작한 블로그로 비트코인을 쓸쓸하게 범
- Bitcoin Magazine 온라인 출판 시작
- 대학교 자퇴, Peter Thiel이 fellowship 해줌
- 비트코인의 한계를 극복하기 위해 연구
- CryptoAnarchists와 바르셀로나 은둔 생활
- 설거지랑 요리 분담한 것도 제대로 안하는 것들.. 역시 보상이 없으면 안됨
- 이메일로 아이디어 소수와 공유
- 이더리움 시작

원본 기사 내용 요약:  
<http://fortune.com/ethereum-blockchain-vitalik-buterin/>

# 이더리움 - SMART CONTRACT

A 가 B 에게 10 BTC를 준다 (단순 화폐 거래)

SMART CONTRACT  
조건문 / if... then... / 계약 코드 / 베팅

만약 이재명이 당선되면 A는 B에게 10ETH를 준다.  
남경필이 당선되면 B는 A에게 10 ETH를 준다.

A가 B 집의 디지털 현관문 IoT에 비밀번호를 제대로 치면  
A 지갑에서 B에게로 100 ETH를 보낸다.

# 이더리움으로 보는 HARD FORK / SOFT FORK

DAO 해킹 사태 이후, 하드포크를 감행  
이더리움(75%) 이더리움 클래식(15%)으로 나눠짐

시스템을 유지 보수 및 규칙 RULE 변경을 위해  
버전 업데이트할 때, 의견 충돌시 ‘파’가 갈리는 것

P.130 비트코인과 블록체인

A  
이전 규칙을  
따르는 노드가  
생성한 블록

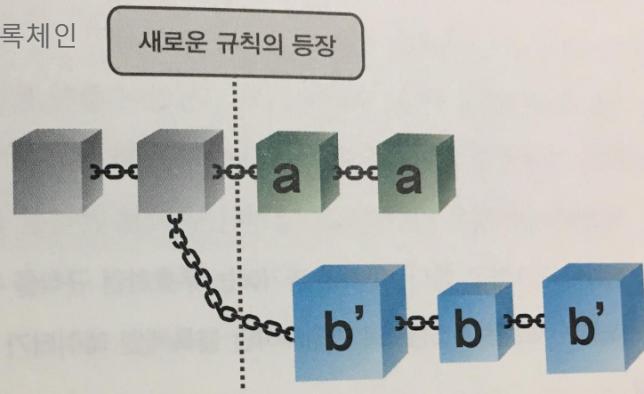
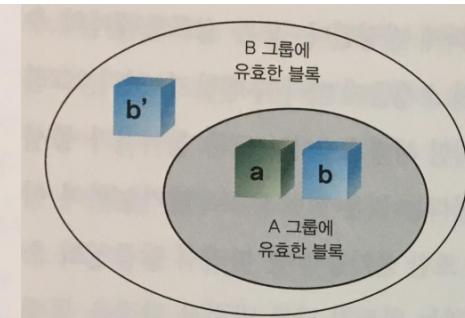


그림 3-19 하드포크의 경우

과거에는 무효하던 규칙을  
유효화한 경우 - 하드포크



과거에는 유효하던 규칙을  
무효화한 경우 - 소프트포크

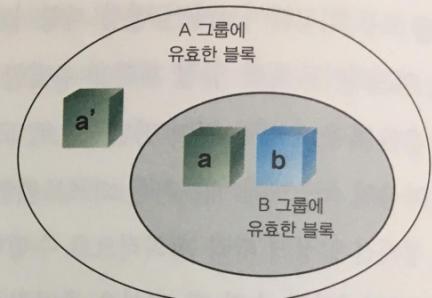


그림 3-18 규칙을 변경할 경우 발생하는 상황

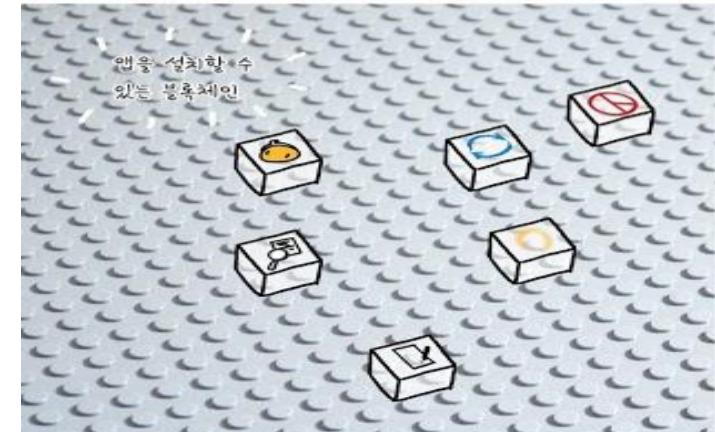
# 이더리움 - DApp

- 플랫폼 철학
- 우리가 지금 쓰고 있는 **스마트폰**처럼  
여러 서비스가 가능한 플랫폼을 구축하자
- ERC 20 Token 규약을 따르면 너와 나의 코인  
모두 이더리움에서 돌아갈 수 있다
- 예) 예측 시장 베팅 앱, 금과 블록체인 거래 앱,  
Hedge Fund 자산관리와 수익구조 투명 특화 앱,  
의료 분야 데이터 관련 앱 (Melonport),  
Airbnb와 IoT와 블록체인을 연결한 숙박 DApp (Slock.it),  
탈중앙화/분산화 방식으로 파일 복구 앱 (swarm),  
신원 블록체인 앱 (uport)



스마트폰 하나에  
다양한 앱을 깔아서 쓰듯이

이미지 출처:  
<https://steemkr.com/webtoon/@leesol/webtoon-gopax-x-leesol-2>,  
<https://imgur.com/7yWyeXj>



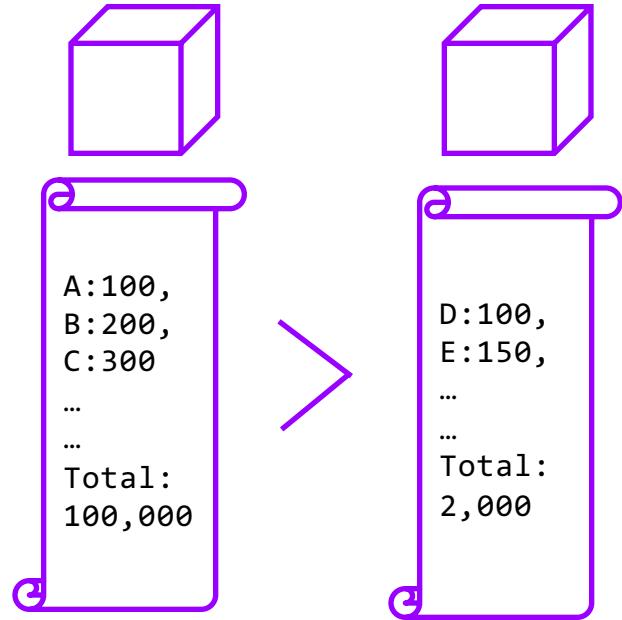
# 이더리움 - PoW → PoS

## □ PoW: Proof of Work: ‘작업량’으로 이 블록을 증명해라

- 여러 블록 후보들이 나왔다면 손이 더 많이 간 블록이 채택된다

## □ PoS: Proof of Stake: ‘재산’으로 이 블록을 증명해라

- ‘이 블록은 유효하다’라는 증명의 싸인을 함
- 여러 블록 후보들이 나왔다면 ‘이 블록이다’라고 싸인한 사람들의 총 재산이 더 많은 블록이 채택된다.



# PoW, PoS, 51%의 공격, 그리고 ...

블록체인을 업데이트 하기 위한 권한을 부여하는 합의 매커니즘	기준	51%의 공격	문제점
<b>PoW Proof of Work 작업 증명</b>	채굴에 들어가는 작업량	<b>전세계 채굴 연산량의 51% 이상을 보유하면 그 시스템을 파괴할 수 있다.</b>	채굴기 가격 폭증, 하드웨어 / GPU / 전력량 대란, 그만큼의 하드웨어 구매 가능한 단체들이 채굴 반 이상 차지
<b>PoS Proof of Stake 지분 증명</b>	이 시스템에서 stake/지분을 많이 가지고 있는 사람들	<b>전세계 자산의 51% 이상을 보유하면 그 시스템을 파괴할 수 있다. (이론상 PoW 51%의 몇백, 몇천배...)</b>	지분이 많을수록 화폐의 가치가 떨어지는 것이 싫으니, 증명에 힘쓸 것. → 하지만 가짜 블록 후보가 들어와도 손해볼 것 없으니 <b>여기저기 다 싸인함.</b> <b>Nothing At Stake</b> → <b>비탈릭: CASPER 제안.</b> 보증금을 맡겨두고 잘못 증명하면 깍는 것.

<내가 소개하는 이번 주 맛집> 큐레이팅이 종료되었습니다. 결과를 확인하세요!!

 tasteem-kr (59) ▾ in tasteem • 12시간 전



## 내가 소개하는 이번 주 맛집

여러분이 아끼는 식당은 어디인가요?

사랑하는 사람을, 장소를, 식당을 기억하지 못하면  
외로워지더라고요.

당신이 이번 주에 갔던 식당 중 가장 편찮았던 곳을,  
예전부터 아껴왔던 곳을,  
앞으로 아끼게 될 식당을 테이스팀에 남겨주세요.



# steemit

이미지 출처:

<https://steemit.com/tasteem/@tasteem-kr/tasteem-event-510eb9>

tasteem contest restaurant kr kr-food

 12시간 전 by tasteem-kr (59) ▾

 \$31.85 ▾ 16 보팅 ▾  댓글 달기 



tailcock (54) ▾ · 12시간 전

갈수록 테이스팀 포스팅의 질이 높아지고 있네요.

 \$0.00 댓글 달기



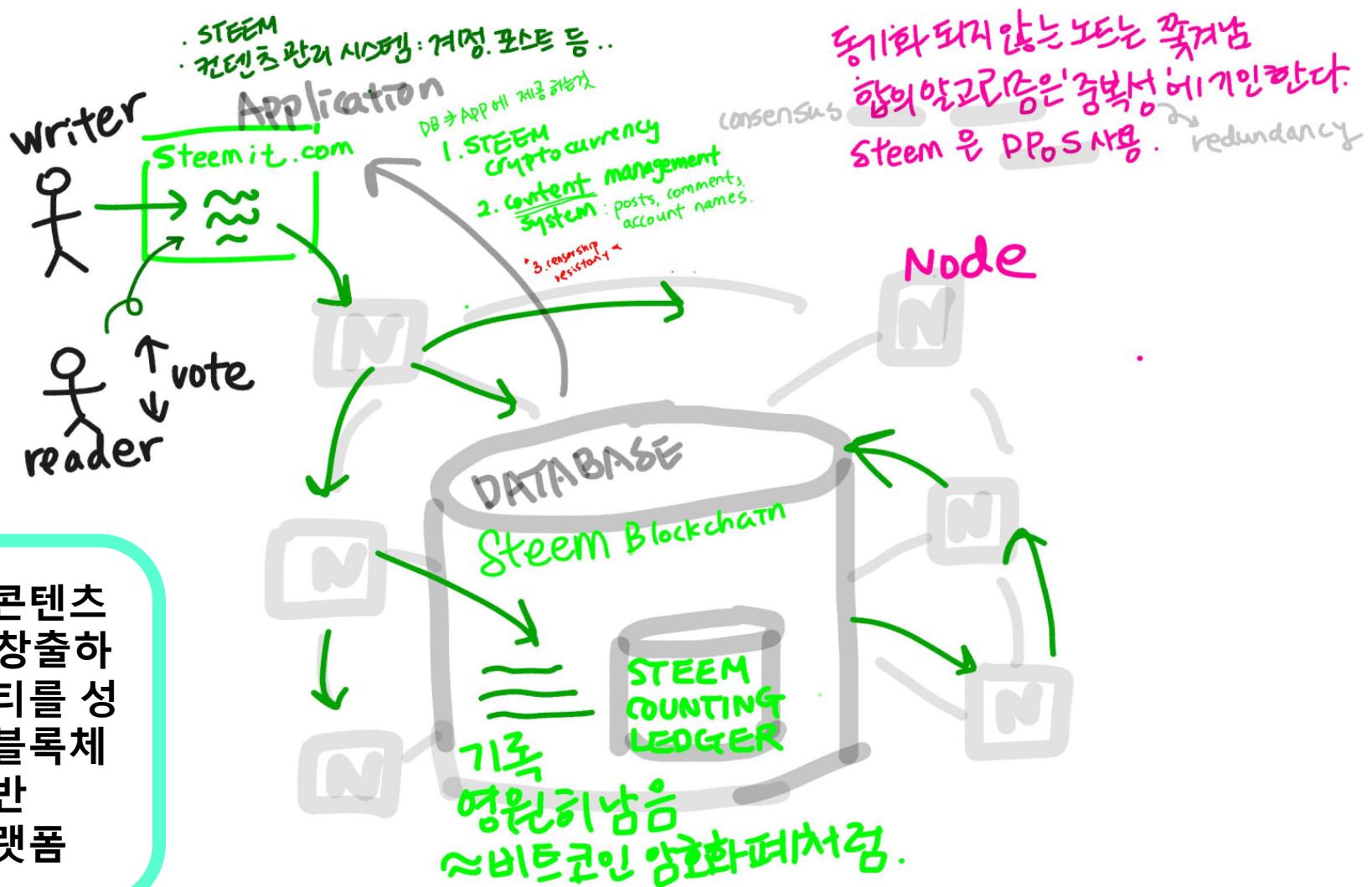
jsj1215 (62) ▾ · 11시간 전

첫 테이스팀 포스팅에서 1등을  
감사합니다~^^

 \$0.00 댓글 달기

# 스팀잇

게시자가 콘텐츠로 수익을 창출하고, 커뮤니티를 성장시키는 블록체인 기반 보상 플랫폼



# 스팀잇 - DPoS

- Delegated Proof of Stake
  - 위임권을 가지는 WITNESS = 증인들 = 고래 (30명)
- 장점
  - 거래 수수료 없음
  - 트랜잭션 확인 속도 향상
  - 높은 대역폭 (현재까지 가장 빠른 체인)
    - \*대역폭: 내가 사용할때 인터넷/네트워크 속도
- PoS vs. DPoS ⇒ Steem에서는 자산에 따라서 대역폭을 할당받는다
  - PoS에서는 내 자산이 적으면 아예 기회조차 없을 수가 있다
  - DPoS에서는 내 자산이 야무리 절어도 약간의 할당량은 보장받는다

# 스팀잇 - 키워드

## □ VOTING

매일 주기적으로 개인당 투표량이 갱신된다.

내가 타인의 포스팅에 VOTE했을 때, 나에게 돌아오는 보상 값도 있다.

이 VOTE가 보상(\$....)이고, 돈으로 환산할 수 있다.

## □ STEEM POWER

STEEM의 지분은 어떻게 상승하냐고 묻는다면,

나의 대역폭을 늘리기 위해 STEEM을 매매한다.

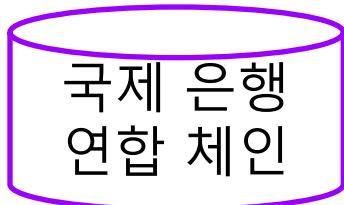
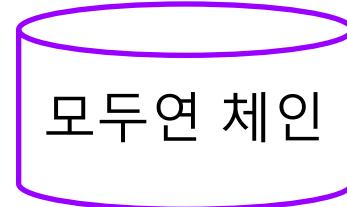
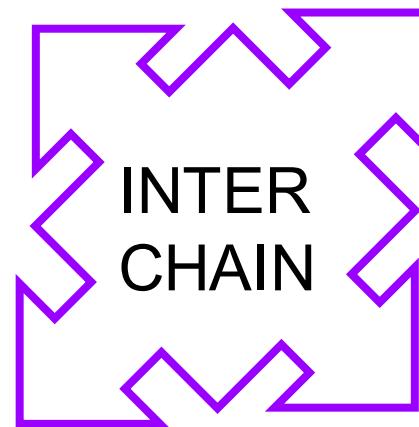
커뮤니티의 성장에 따라 화폐 가치가 상승할 것이다.

## □ STEEM Dollar

## □ Graphene Protocol

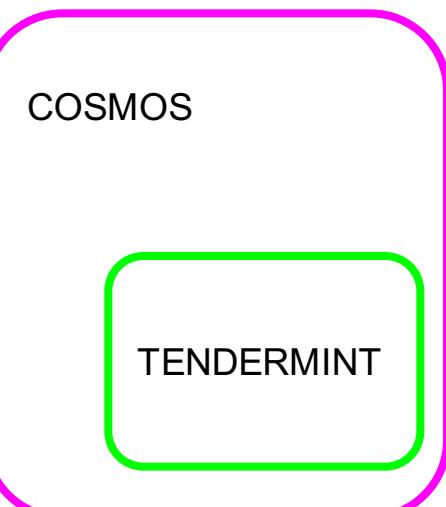
## □ Bloom Filter

# 인터체인 INTERCHAIN



# 인터체인

- ❑ 인터체인 회사들
  - ❑ COSMOS
  - ❑ ICON
  - ❑ AION
- ❑ COSMOS: Jae Kwon 설립 (유튜브 인터뷰)
- ❑ INTERCHAIN Foundation
  - ❑ 블록체인계의 인터넷을 꿈꾼다
- ❑ TENDERMINT: COSMOS가 쓰는 합의 알고리즘
  - ❑ 비잔틴 장군 문제 기반



# 인터체인

- ❑ 인터체인 회사들
  - ❑ COSMOS
  - ❑ ICON
  - ❑ AION
- ❑ COSMOS: Jae Kwon 설립 (유튜브 인터뷰)
- ❑ INTERCHAIN Foundation
  - ❑ 블록체인계의 인터넷을 꿈꾼다
- ❑ TENDERMINT: COSMOS가 쓰는 합의 알고리즘
  - ❑ 비잔틴 장군 문제 기반

INTERCHAIN FOUNDATION

COSMOS

TENDERMINT

# 블록체인 공부 흐름

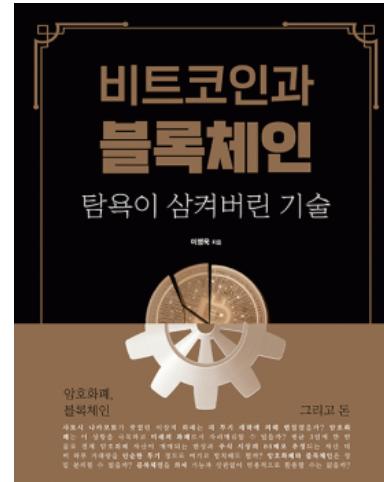
- TED 영상:

[https://www.ted.com/talks/bettina\\_warburg\\_how\\_the\\_blockchain\\_will\\_radically\\_transform\\_the\\_economy](https://www.ted.com/talks/bettina_warburg_how_the_blockchain_will_radically_transform_the_economy) (How the blockchain will radically transform the economy, Bettina Warburg)

- 비트코인과 블록체인: 탐욕이 삼켜버린 기술 책 (저 이병욱)
- 블록체인 애플리케이션 개발 실전 입문 책
- 스팀잇 밋업, EOS 밋업, 스팀잇 스터디
- ICO 블록체인 포럼
- 유튜브 Studio Decentral 등 강의 컨텐츠

# 블록체인 공부 팁

- 사회 경제적 관점에서의 블록체인 유의미성에 대한 강연 영상
- 비트코인과 블록체인 책 (저 이병욱), 유튜브 Studio Decentral, Steemit 이솔 블록체인 웹툰 등 다가가기 쉬운 블록체인 강의 컨텐츠
- 이더리움, Cosmos 등 블록체인 플랫폼 founder 들의 인터뷰 영상
- 신뢰할만한 언론사의 블록체인 뉴스 기사들
- 이더리움 기술 실습서
- 블록체인 백서들, 밋업, 세미나 등



[Webtoon][GOPAX x LEESOL] 알면 쉬운 블록체인 시즌 2-2화. 암호화폐를 분류해보자

leesol (66) · in webtoon · 5개월 전



GOPAX x leesol

웹툰  
▼  
알면 쉬운 블록체인 시즌2

2화. 암호화폐를 분류해보자.



# 블록체인 공부 팁

- 사회 경제적 관점에서의 블록체인 유의미성에 대한 강연 영상
- 비트코인과 블록체인 책 (저 이병욱), 유튜브 Studio Decentral, Steemit 이솔 블록체인 웹 툰 등 다가가기 쉬운 블록체인 강의 컨텐츠
- 이더리움, Cosmos 등 블록체인 플랫폼 founder 들의 인터뷰 영상
- 신뢰할만한 언론사의 블록체인 뉴스 기사들
- 이더리움 기술 실습서
- 블록체인 백서들, 밋업, 세미나 등

https://www.kci.go.kr/kciweb/search/searchResultView.do?idx=111  
한국과학기술정보연구원(KCI)은 대한민국 과학기술 정보를 수집·보관·제공하는 학술정보 서비스기관입니다.



## 블록체인

애플리케이션 개발 실전 입문

Solidity를 이용한 이더리움 스마트 계약 구현



core ethereum  
p r o g r a m m i n g  
코어 이더리움 프로그래밍  
블록체인, 이더리움 핵심에서 암호화폐 구축을 위한 스마트 컨트랙트 개발까지