Consensus Mechanisms in Major Cryptocurrencies

Lecture in B-Capitalist Course

이흥노, GIST, South Korea
Home page: http://infonet.gist.ac.kr
Facebook/Publication ID: Heung-No Lee
E-mail: heungno@gist.ac.kr

Agenda of this talk

- 강사소개
- Bitcoin Consensus
- Other Consensuses

이흥노 교수

GIST **블록체인 인터넷 경제연구센터 / 센서지능화센터 센터장**

LiberVance 리버밴스㈜ 설립자

GIST 이흥노

국가스마트도시위원회 민간위원, (사)대한전자공학회 통신소사이어티 회장
우정사업본부 블록체인이니셔티브 민간위원

연구실적

- **국제 논문 (SCI) : 200+편(71+편)**
- 국제 특허 : 출원 9건, 등록 7건
- 국내 특허 : 출원 7건, 등록 22건
- **기술이전 : 2건 (2억 1천만원)**
- 저술 : 8건
- 기술가치평가 : 1건(중앙기술평가원)

대표언론보도

- 프레시안, "GIST, 글로벌 블록체인 개발회사 '컨센시스' 와 MOU" (2019.07.21)
- 스마트시티랩, "블록체인 스마트시티의 유기적 연결의 중추 역할 할 것" (2018.08.24)
- 전자신문, "대한전자공학회 통신소사이어티(회장 이흥노), 19일 블록체인으로 여는 미래' 워크숍 개최" (2018/04/16)
- 블록체인허브, "블록체인·AI·빅데이터 융합산업 육성 정책토론회", (2018/12/06)

연구분야

- 블록체인경제
- 지능형 네트워크
- 센서지능화

관련수상이력

- **2019년 대한전자공학회 해동학술상 수상**
- 2016년 GIST 연구상
- **2016년 GIST 대표기술상**
- **2014년 1월 이달의 과학기술자상, 미창부**
- 2013년 기초연구 우수성과 50선, 미창부
- **2012년 국가연구개발 우수성과 100, 미창부**

보유기술현황

보유기술

- GIST는 블록체인의 재중앙화 문제 해결을 위한 **부호-암호 기반의 작업증명** 방식 연구 및 특허 확보 및 출원한 **부호-암호 작업증명 특허**
  (GIST IP)를 기반으로 블록체인 시스템 개발

특허

특허	출원인	출원번호/등록일	핵심기술
부호-암호 화폐 시스템	광주과학기술원	10-2019-0151246 / 2019.11.12	블록체인의 재중앙화 문제 해결을 위한 핵심 기술
블록체인거버넌스	광주과학기술원	10-2019-0084800 / 2019-07-12	블록체인 거버넌스와 규제
블록체인의 거래검증시스템, 및 블록체인이 거래검증방법	광주과학기술원	10-2019-0120655 / 2019-09-30	블록체인거래검증

Consensus

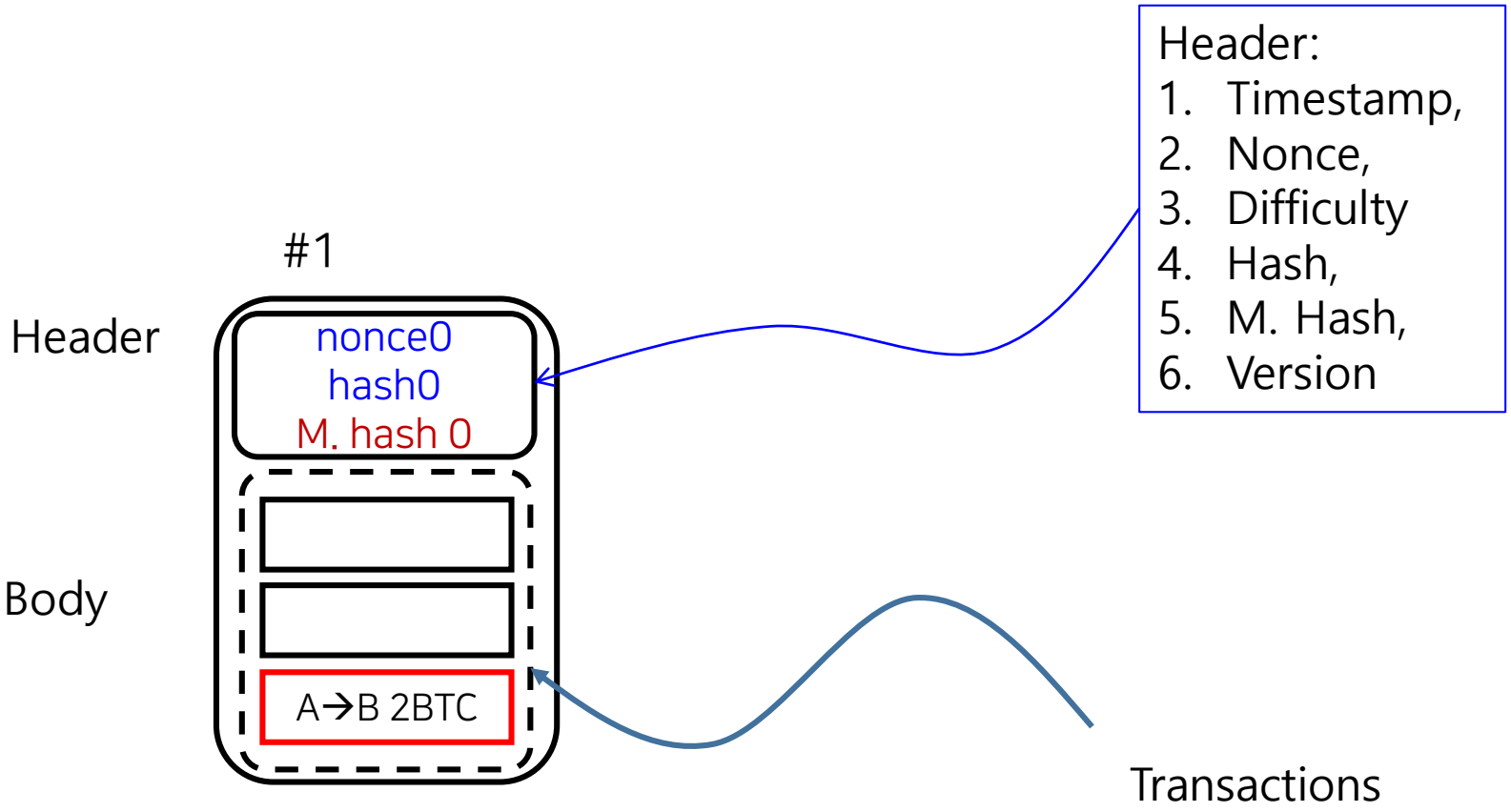
- **Goal: 하나의 동일한 원장 유지 관리**

- Nodes: 글로벌 영역에 분산되어 있는 노드 N개
  1. State: 각 노드의 현재 상태
     A. Work: (각자) 새로운 TXs 담아 블록 생성
     B. Announce: 발표
     C. Inspection: 검사
     D. Approval: 승인
  2. State Update: 새로운 블록을 기존 블록체인에 순서대로 추가

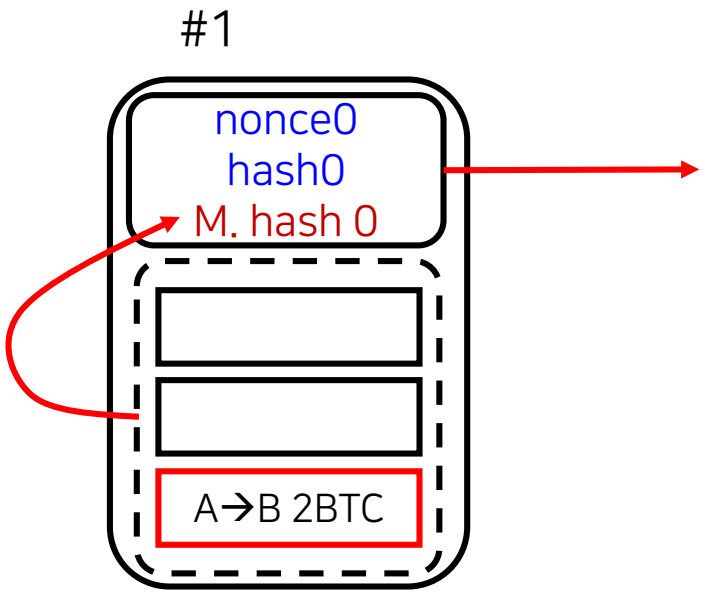
Consensus Algorithm설계의 어려움

- 노드들은 인터넷 상에서 협력하여 합의에 도달해야 함
- OS SW
- Cryptocurrency의 경우 다양한 공격 방법이 존재
  - Sybil Attack
  - DDoS Attack
  - Byzantine faults

Block: Header 와 Body



Secure Hash Function: 블록요약을 만드는 함수



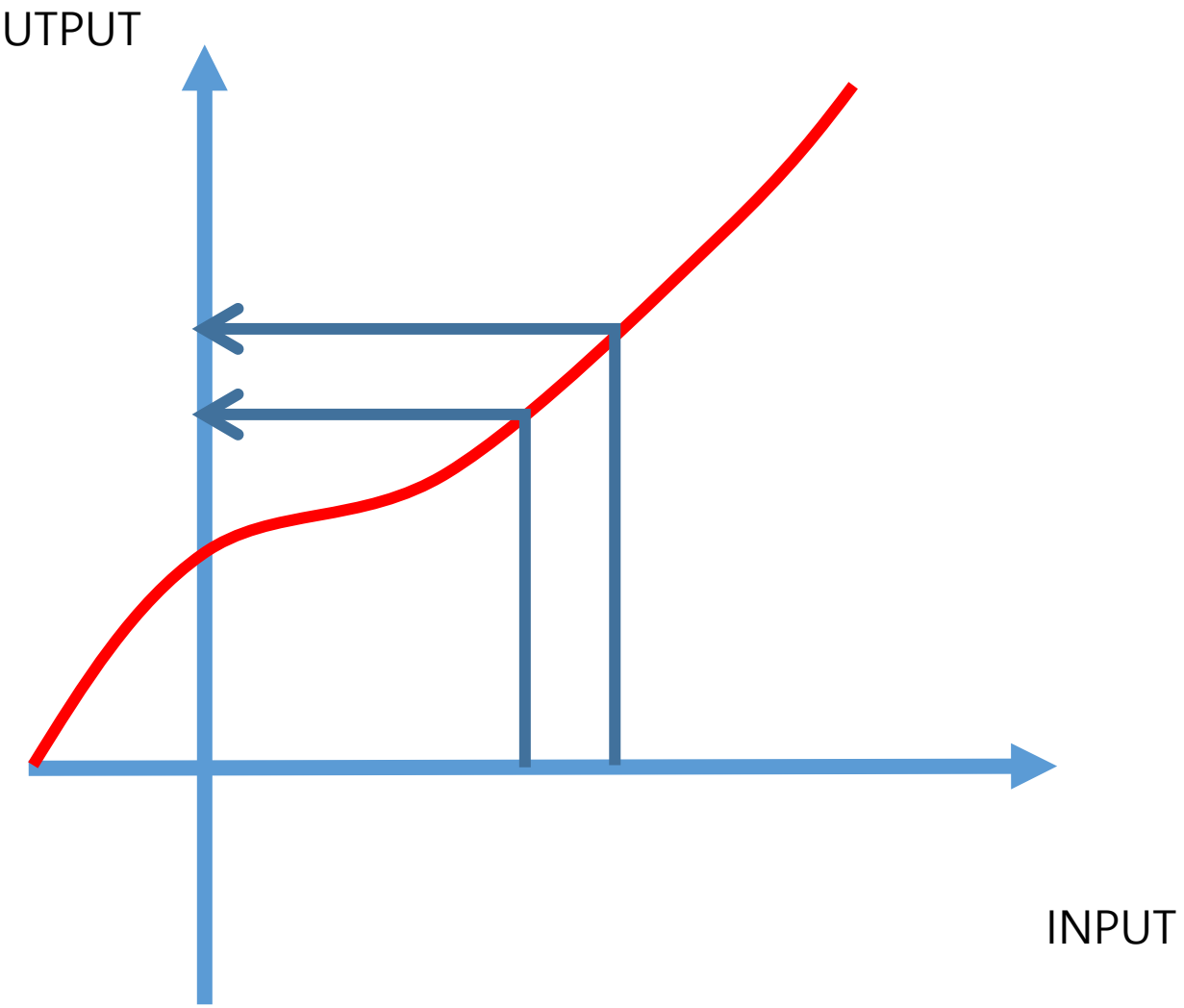
특징: Oneway 앞으로만 가는 함수.
뒤로 가려면 대입법 밖에 없다.

함수는 INPUT 을 받고 OUTPUT을 만든다
INPUT: 파일
OUTPUT: 256 bit 숫자

쓰이는 곳
1. 은행 서버는 Passwd의 hash값만 저장해 놓는다.
2. Spam mail 방지
3. PoW

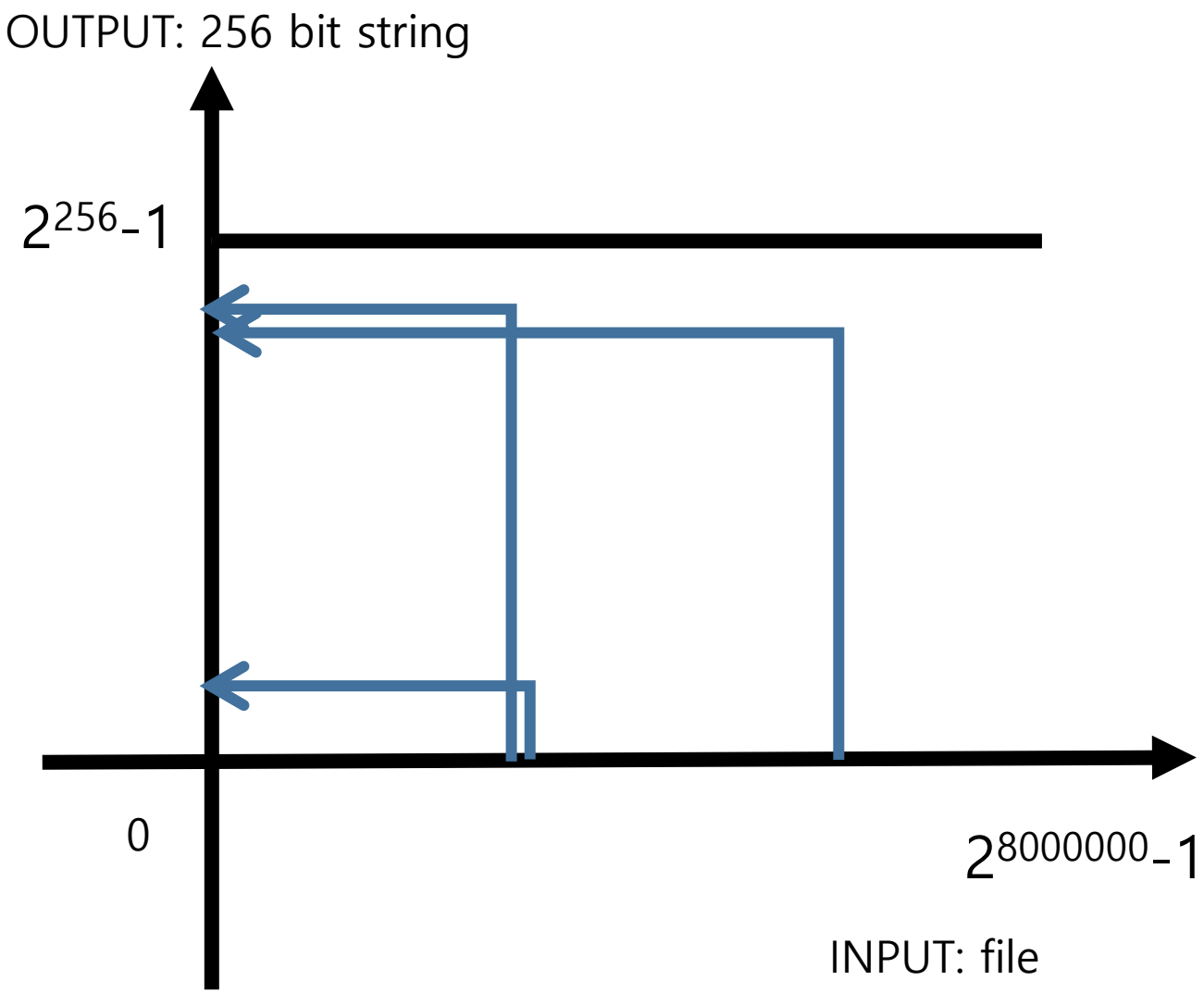
일반 함수

- Output을 본 후,
  Input 예측 가능함



SHA 함수

- 동일한 Input은 언제나 동일한 Output 출력.
- Input이 조금만 차이가 나도, 마치 무작위로 선택된 것 같은 Output을 줌.
- 결과: Output 값을 얻은 후 Input값을 전혀 예측 할 수 없게 됨.
- Many to 1 함수, but collision free!



Modulo Operation

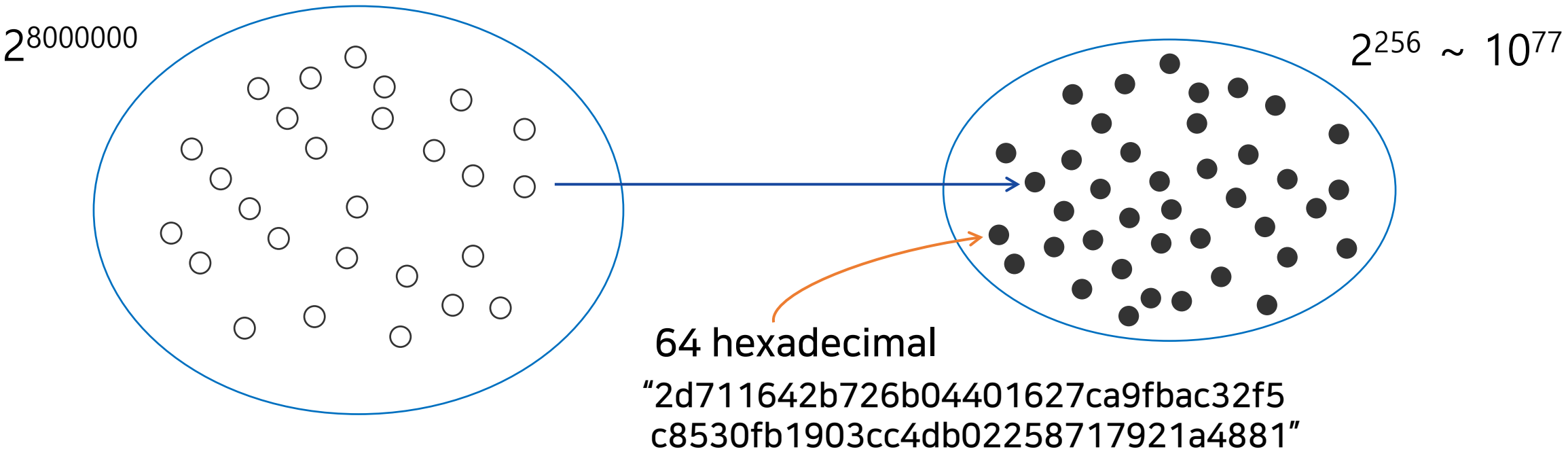
- F(x) = y
- F(x) = 7x + 6 mod 5

- Let x = 5. Then, y = 7*5 + 6 = 41 mod 5 = 1.
- Let x = 4. Then, y = 7*4 + 6 = 34 mod 5 = 4.

Hash 함수

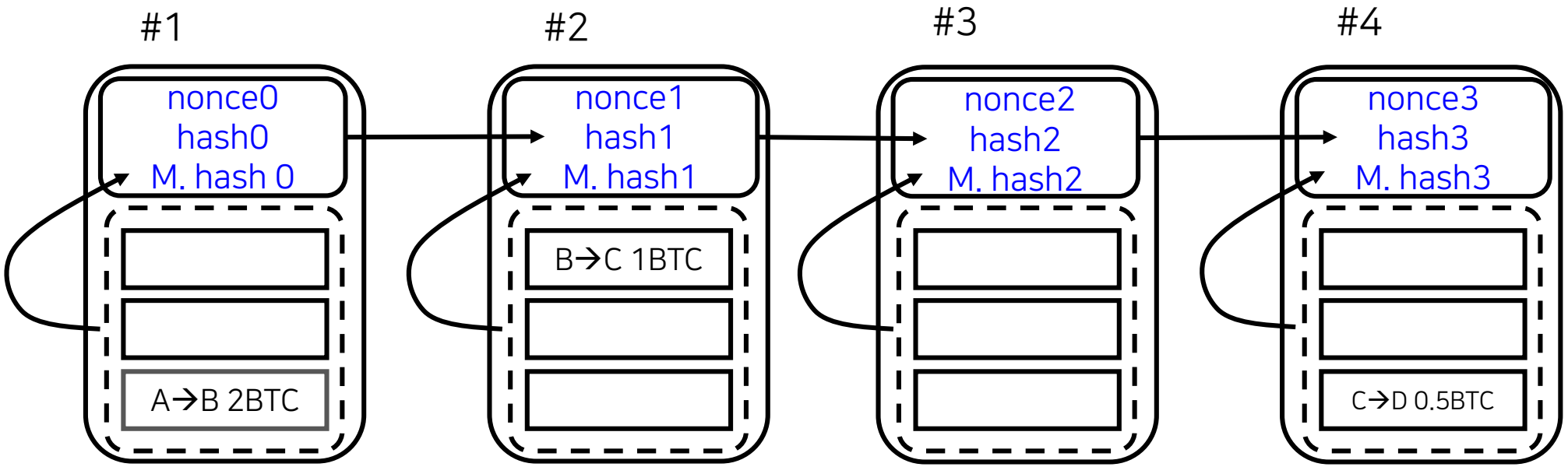
- SHA256, $F(x) = y$

$X = \{x | x \text{ is a message up to 1 Mbyte in size}\}$ $Y = \{y | y \text{ is a 256bit string}\}$

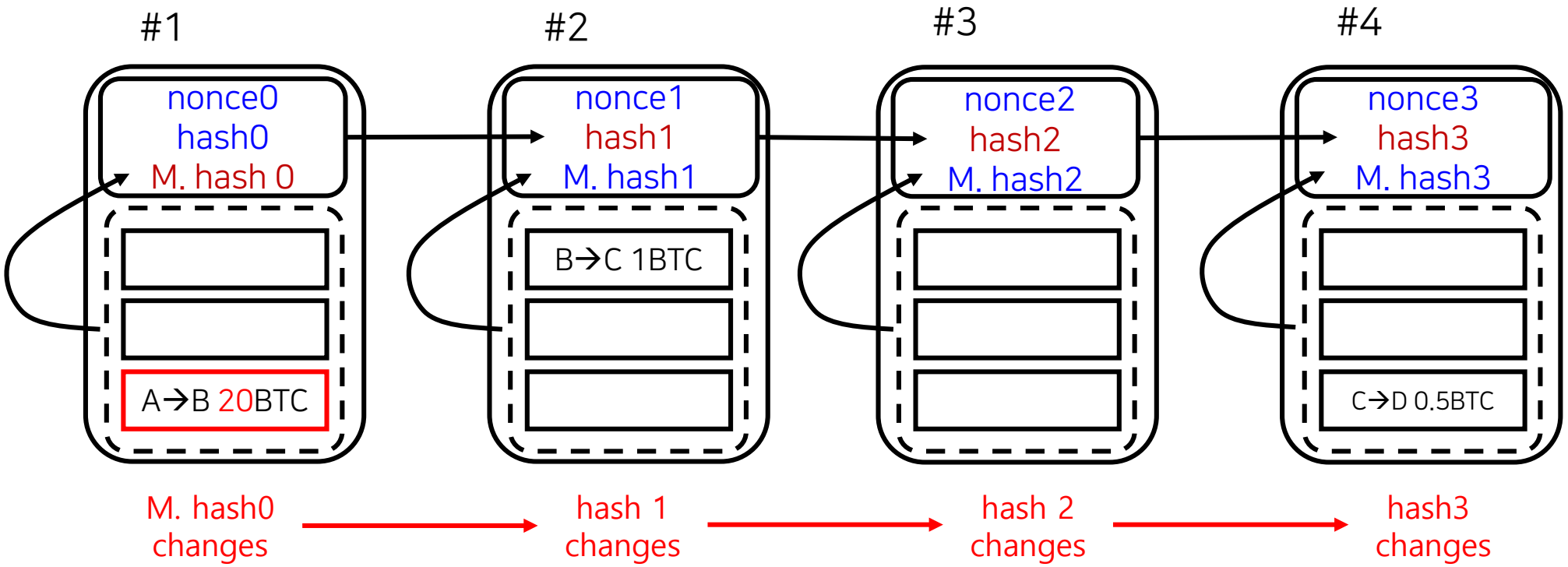


Blockchain이란?

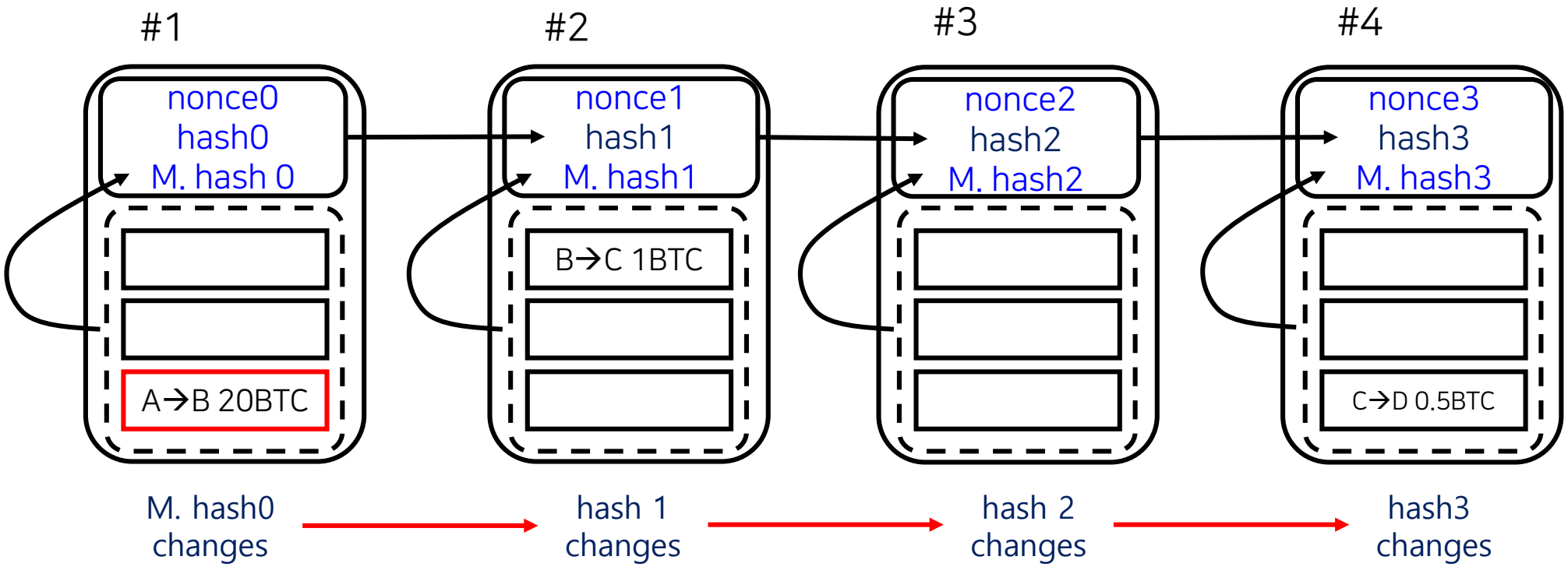
- Block body의 hash값을 Block header에 넣고
- Oneway function으로 block 과 block을 연결하는 것



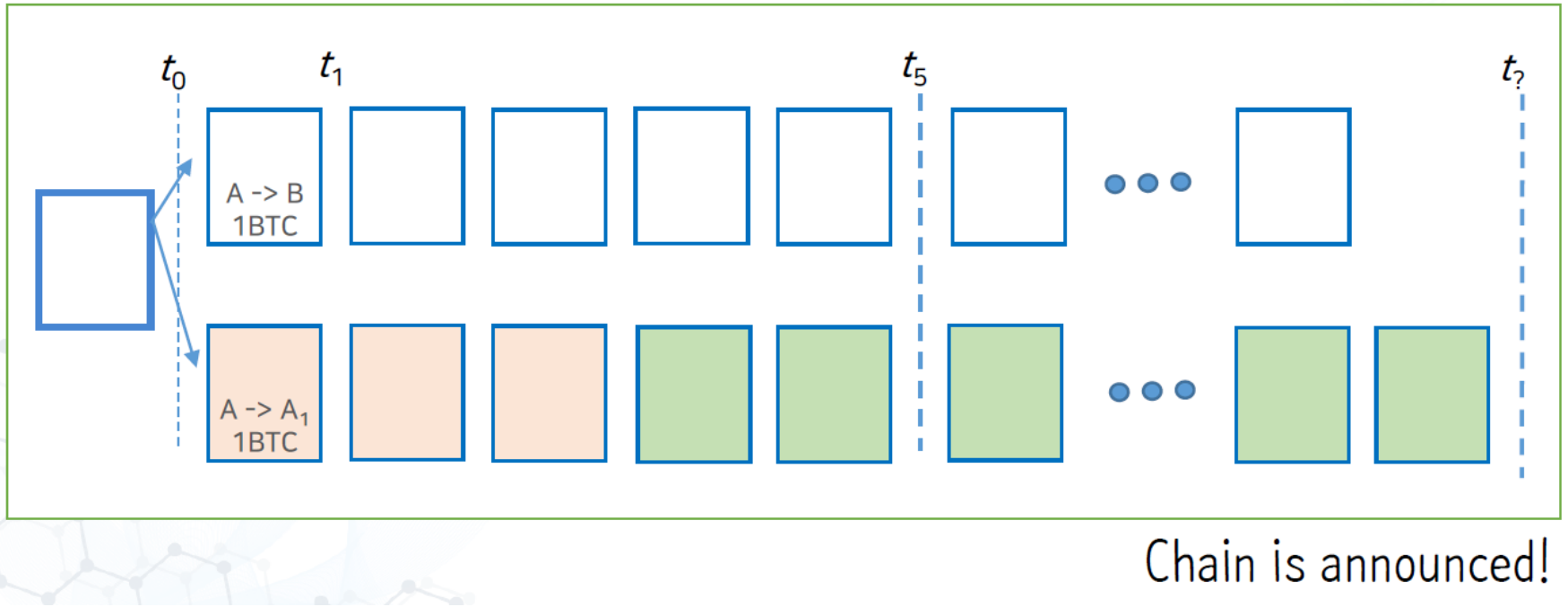
Block을 Chain으로 연결하여 얻는 효과는?



Block을 Chain으로 연결하면 컨텐츠를 못 바꿀까?

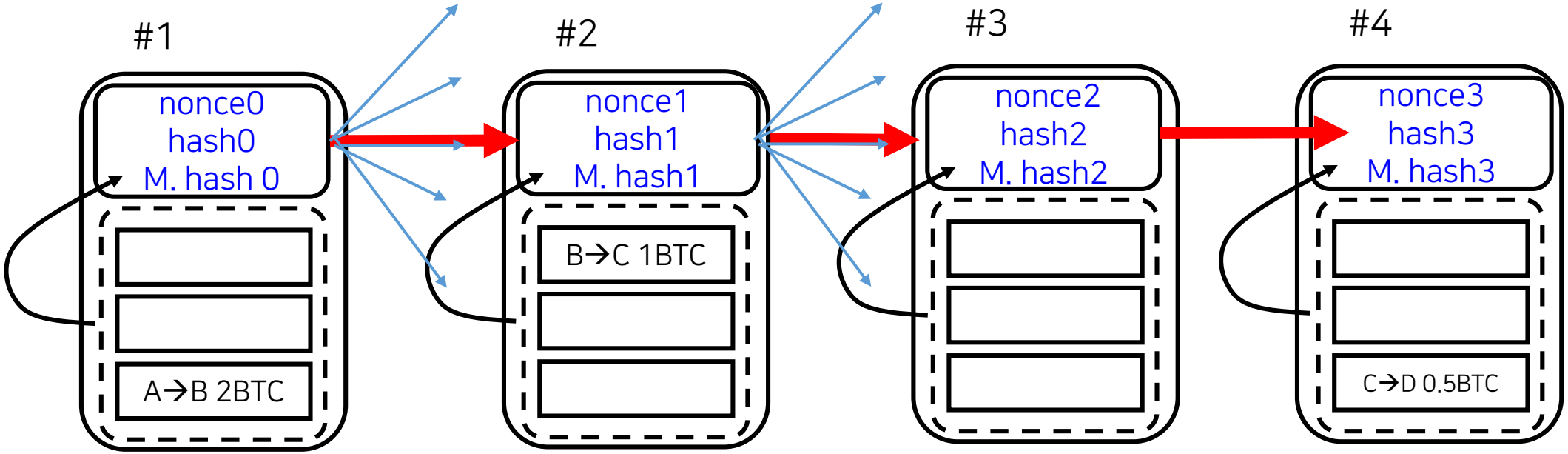


Double Spending은 어떻게 성립하는가?
방지하려면 무엇이 필요한가?



자세한 내용은 이 링크를 눌러 확인하세요 https://arxiv.org/abs/1903.01711

컨텐츠를 바꿀 수 없게 하려면 무엇이 필요한가?



- Block Chain + PoW
  - Revolutionary new idea!
    - Al-Im-To-Po Theory!
    - The more come to get involved, the safer the network becomes!
    - Reward
    - Fresh new race for each block.
    - Race means competition.

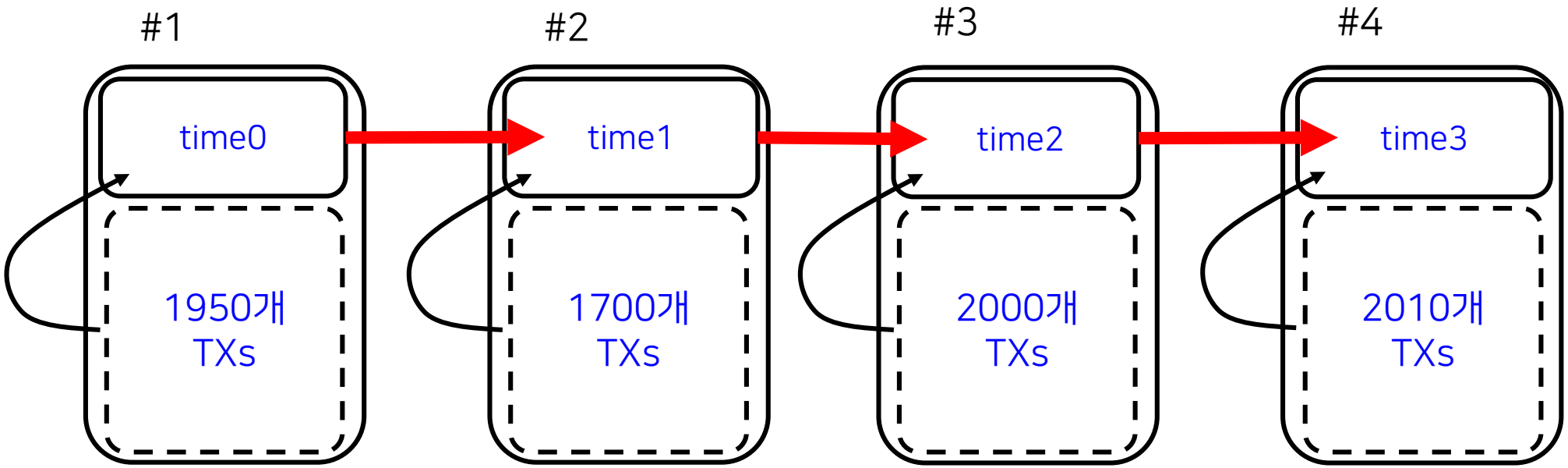
Block #613573

BlockHash 00000000000000000000288ae77f5b8b3c99784f55827431a23f524adf69d0e3a

Summary

Number Of Transactions	3170	**Difficulty**	14776367535688.639
Height	613573 (Mainchain)	**Bits**	17130c78
Block Reward	12.5 BTC	**Size (bytes)**	869316
Timestamp	Jan 20, 2020 1:15:17 AM	**Version**	1073733632
Mined by		**Nonce**	3774951927
Merkle Root	523c52ad89c6ac67bcc01a6...		
Previous Block	613572		

Block Interval, TXs/Block, TPS



TPS = TXs/Block / BI
= 2000 TXs/600초
= 3.3 TXs/sec

TPS제고 필요성 제기

- 인기가 많은 블록체인에만 해당
- TPS를 높이려면?
  1. 블록사이즈를 키우거나
  2. 블록인터벌을 줄이거나
  3. Both

블록인터벌 **BI** 을 줄이려면?

- 노드 수를 줄이는 프로젝트들이 성행
  - 적은 수의 노드에서 잘 돌아가는 합의알고리즘 사용

  - 그러나 노드 수가 적으면
    - 탈 중앙화는????
    - DS 공격 취약성은???
    - Sybil Attack 취약성은???

블록인터벌 **BI** 을 줄이려면? (2)

- PoW도 Block Interval을 줄일 수 있음
  - Litecoin: 2.5분
  - ETH: Block Interval 14초

  - 수 많은 fork가 매 번 발생하는 문제 발생
    - DS 공격 취약성은???
    - 그러나, Profitable DS Attack분석으로 해결 가능 (See DeSecure블록체인)

PoW Puzzles

- Making PoW puzzles
  - Bitcoin uses SHA256.
  - SHA is *oneway* and *collision free*.
  - Difficulty and Nonce are in the BH.

2 PoW Puzzles

- Finding Good Block Summary
  - Function F takes input x and gives output y :

$$y = F(x)$$

  - x is block header (BH), i.e., F(BH) = hash.
  - Then, it can be written as

F(BH: nonce) < Target PoW Ineq.

  - For a block, find a nonce that satisfies the above inequality (Work)
  - Record the nonce in the block header. (Proof)

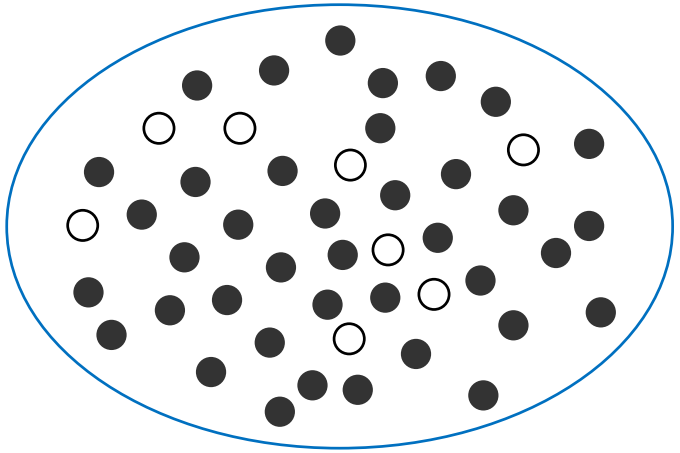
2 PoW Puzzles

- Toy puzzle
  - White and black balls.
  - There are 2^6 balls.
  - Balls are numbers, i.e., hashes.
  - Let Target be 2^3=8.
  - Pick a nonce and run SHA-256.

Total no. of balls $2^6 = 64$
Target = 2^3 0 0 1 0 0 0
White balls = {Balls < Target}
$2^3 - 1 = 7$ 0 0 0 1 1 1
6 0 0 0 1 1 0
5 0 0 0 1 0 1
…

What is the probability that a while ball is picked?

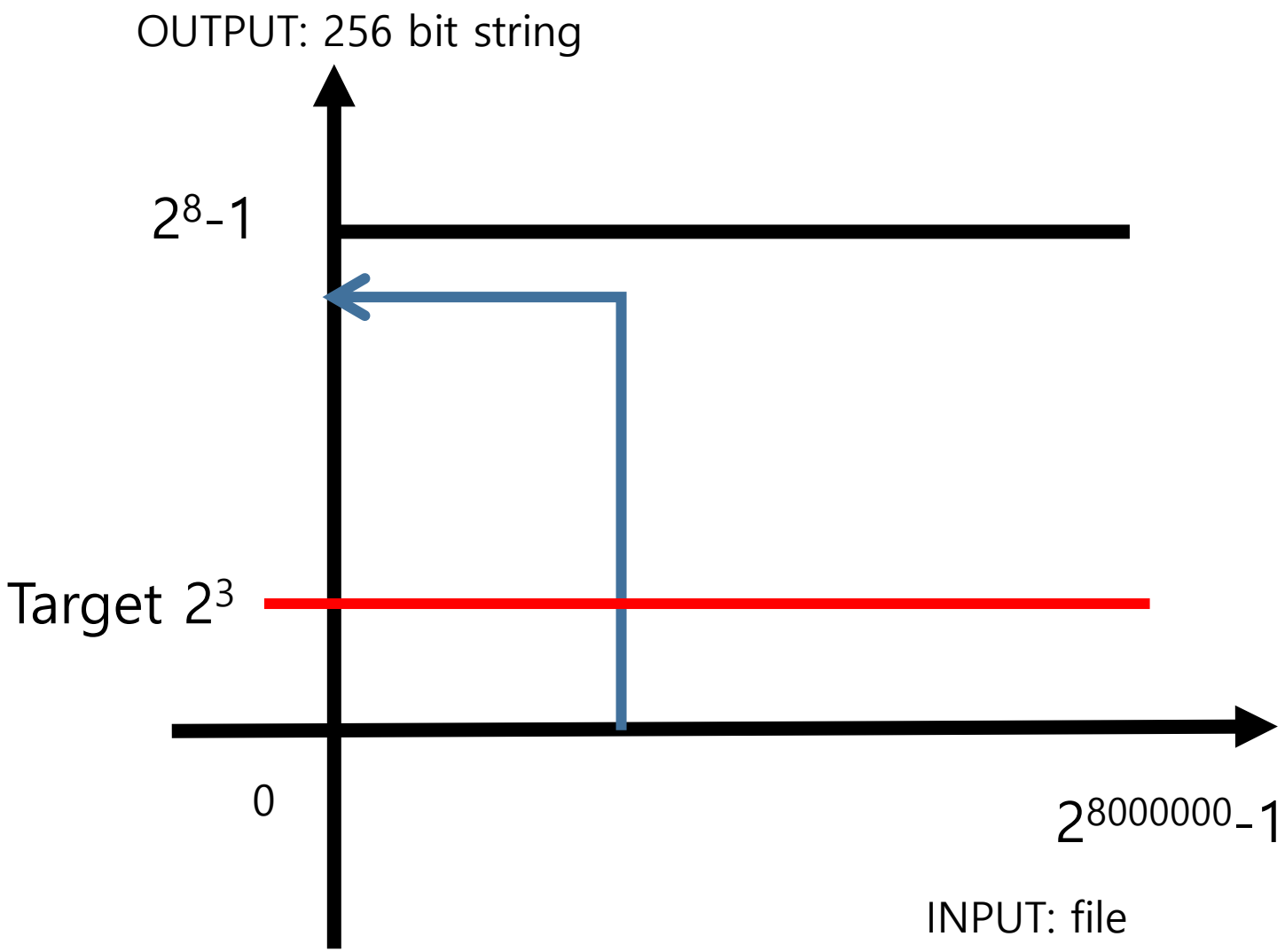
$$p = 2^3/2^6 = 1/8$$



Toy PoW 문제

- SHA-8 사용
- PoW 성공
  - Hash가 8 보다 작은 수가 되는 Input을 찾으면 성공
- 한번 뽑고 PoW 성공 확률?

$$p = 2^3/2^6 = 1/8$$



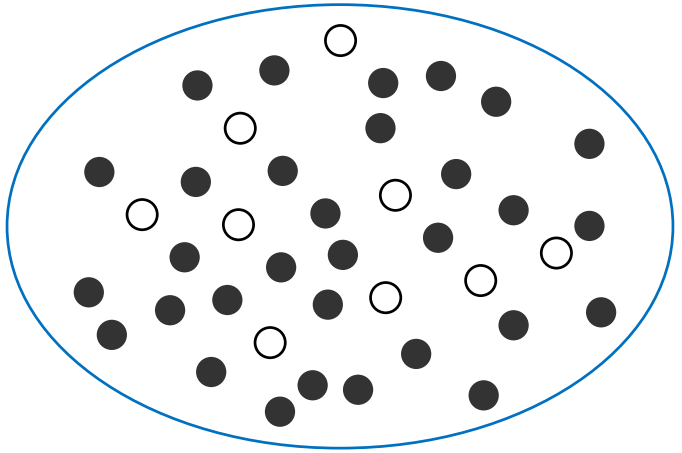
2 PoW Puzzles

- Bitcoin puzzle
  - Hashes are strings of 256 bits.
  - There are 2^{256} hashes in Y.
  - Let Target be $2^{256-16}=2^{240}$.

What is the probability that the hash satisfies the PoW?

$$p = 2^{240}/2^{256}$$
$$= 2^{-16}$$
$$= 1/64000$$

$$Y = \{y | y \text{ is a 256bit string}\}$$



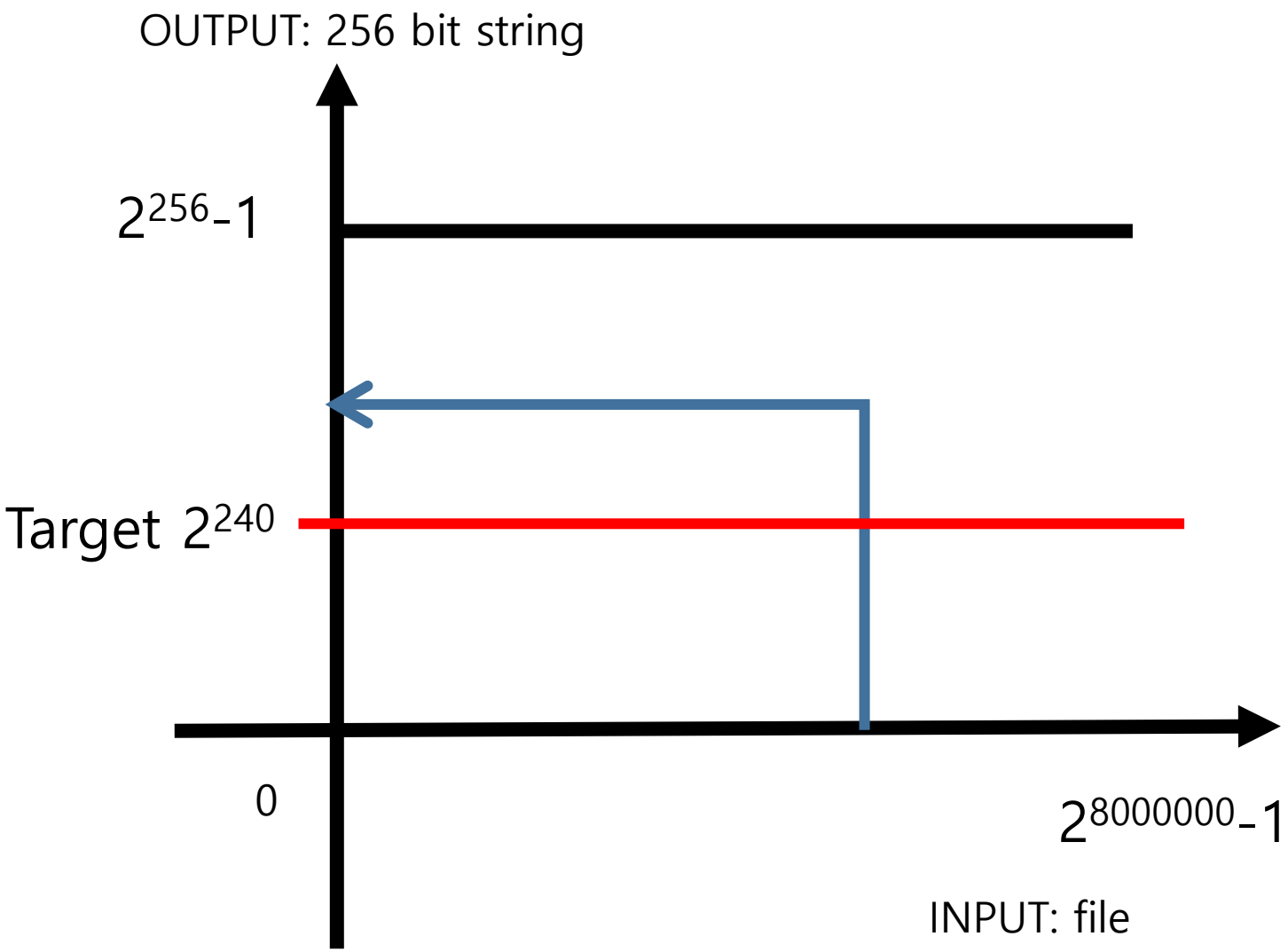
White balls are
64 hexadecimals with 4 leading zeros

"00001642b726b04401627ca9fbac32f5
c8530fb1903cc4db02258717921a4881"

PoW

- SHA-256 사용
- PoW 성공
  - Hash 값이 2^{240} 보다 작은 Input 을 찾으면 성공
- 한번 뽑고 PoW 성공 확률?

$$p = 2^{240}/2^{256}$$
$$= 2^{-16}$$
$$= 1/64000$$



4 Probability of Mining Success

- Given the difficulty p, we aim to find Probability of Mining Success.

- 한 번 뽑을 때 PoW성공 확률이 p 일 때,
  1. k 번째 뽑았을 때 비로서 성공할 확률은?
  2. 평균적으로 몇 번 뽑아야 성공할까?

4 Probability of Mining Success

- (PMF) What is the probability that a CPU solves PoW exactly at the k-th hash?

$$
\begin{aligned}
P_{pmf}(p,\ k) &:= P_p\{K \le k\} - P_p\{K \le k-1\} \\
&= P_p\{K = k\} \\
&= p + (1-p)\,p + (1-p)^2\ p + \cdots + (1-p)^{k-1}\ p \\
&\qquad -\left(p + (1-p)\,p + (1-p)^2\ p + \cdots + (1-p)^{k-2}\ p\right) \\
&= (1-p)^{k-1}\ p \qquad \text{for any } k = 1, 2, 3, \cdots
\end{aligned}
$$

4 Probability of Mining Success

- Average no. of hashes for a PoW success.
  - What is the average number of hashes for a PoW success for a given puzzle difficulty p?

$$\mathbb{E}\{K\} = \sum_{k=1}^{\infty} P_{pmf}(p,\ k)\ k$$

$$= \sum_{k=1}^{\infty} (1-p)^{k}\ p\ k$$

$$= \frac{1}{p}$$

$$= 2^{16} \quad [\text{hashes/block}]$$

Probability of Mining Success

- Definition: Hash Rate of CPU.
  - The hash rate of a CPU is defined as number hashes in a unit time.
  - For example, the hash rate of a CPU which can do 10^6 hash cycles per second is 10^6 hashes/sec.

4 Probability of Mining Success

- ASIC Mining Hardware

Bitcoin Mining Hardware Comparison

Pic	Miner	Hash Power	Price	Buy
	Antminer S9	14.0 TH/s	$3,000	
	Antminer R4	8.6 TH/s	$1,000	

출처: https://www.buybitcoinworldwide.com/mining/hardware/

Bitcoin 난이도 조절

- 평균 **BI**을 10분으로 유지하기 위해 Target값을 조절함

- 문제
- **마이너노드**의 수가 증가하면
  - Network Hash Rate이 낮아/높아 진다.
  - Block Interval이 줄어/길어 진다.
  - 평균 10분 BI을 유지하기 위해서는
  - Target을 크게/작게 해야 한다.

1 Bitcoin Difficulty

- Bitcoin Difficulty (D)

  - The aim is to keep the average block generation time be 10 min.
    - Ex) The time span to mine 2016 blocks is set to take 2 weeks.
  - Difficulty is adjusted for every 2016 block.
  - Measure the time span, T [min], during which the past 2016 blocks were mined.
  - Let T_D be 2 weeks [min], i.e., T_D = 2016x10 = 20160 [min].
  - If T is different from T_D, adjust the Difficulty D :

$$D = D_{prev} \times \frac{T_D}{T}$$

In Bitcoin, initial D is set to 1 with 8 leading hexa zeros.

- Given a Target, one can determine the network hash rate.
- Suppose you bring your own mining chip.
- You can determine your chance of winning a puzzle.
- It is the ratio of your hash rate to the total hash rate:

$$= \frac{\text{Your Hash Rate}}{\text{Your Hash Rate} + \text{Network Hash Rate}}$$

Bitcoin Difficulty

Ex

- Target 이 2^{204}.
- 채굴에 1 Tera hash/sec mining chip을 구매하여 참여.
- 이때 내가 이길 확률은?
  - The network hash power is $2^{256-\log 2target}/600 = 2^{52}/600 = 7.51e12$ [hash/sec].
  - The hash rate percentage is:

$$= \frac{\text{Your Hash Rate}}{\text{Your Hash Rate} + \text{Network Hash Rate}}$$

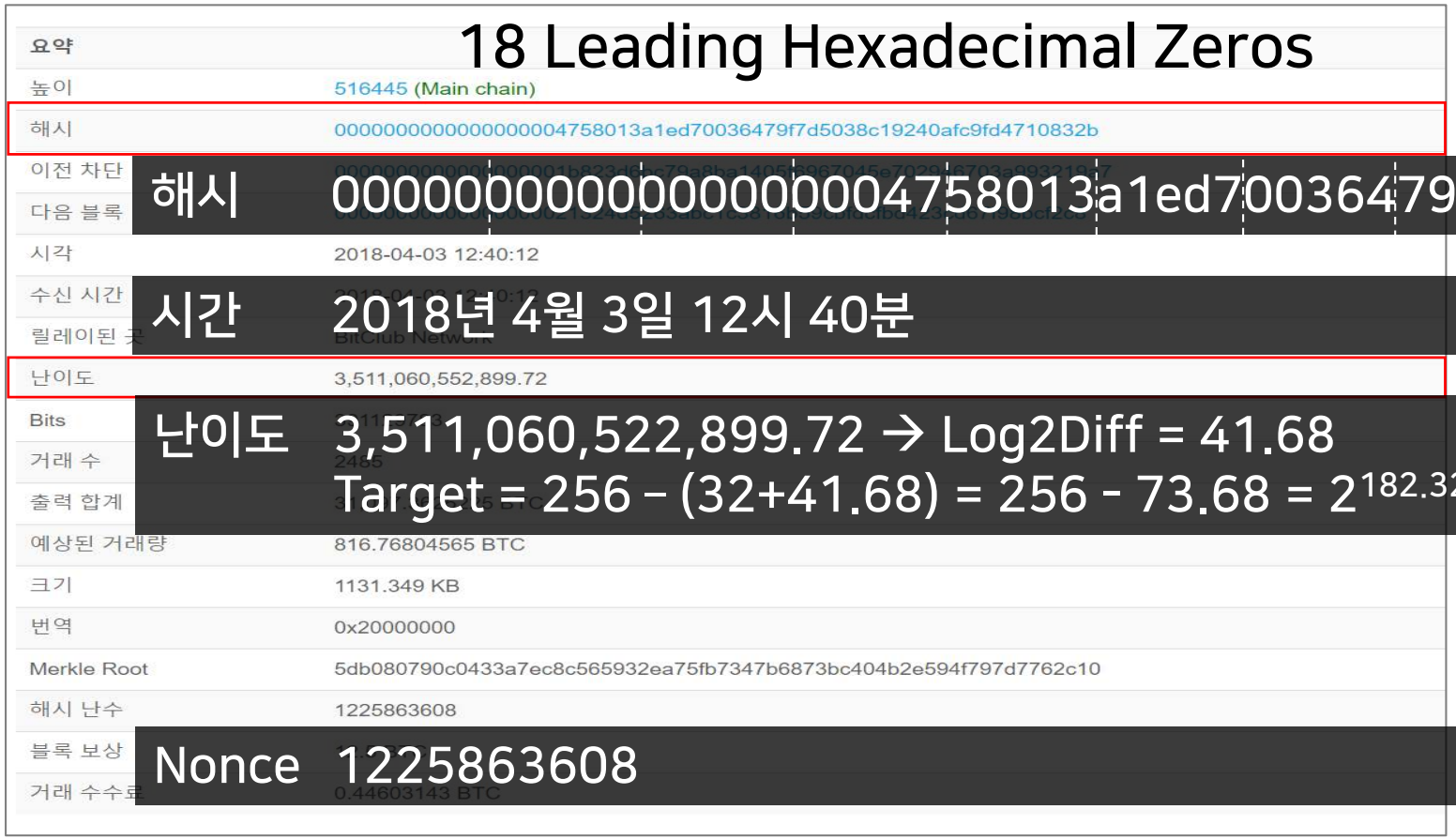
$$= \frac{1.00e12}{1.00e12 + 7.51e12}$$

$$= 11.8\%$$

Bitcoin 실전 문제

Bitcoin Difficulty

- 블록 높이 516445 비트코인 블록체인 내 깊이 값 513445에서의 블록들



18 Leading Hexadecimal Zeros

해시 000000000000000000047580l3a1ed70036479f7d5038c19240afc9fd4710832b

시간 2018년 4월 3일 12시 40분

난이도 3,511,060,522,899.72 → Log2Diff = 41.68
Target = 256 – (32+41.68) = 256 - 73.68 = $2^{182.32}$

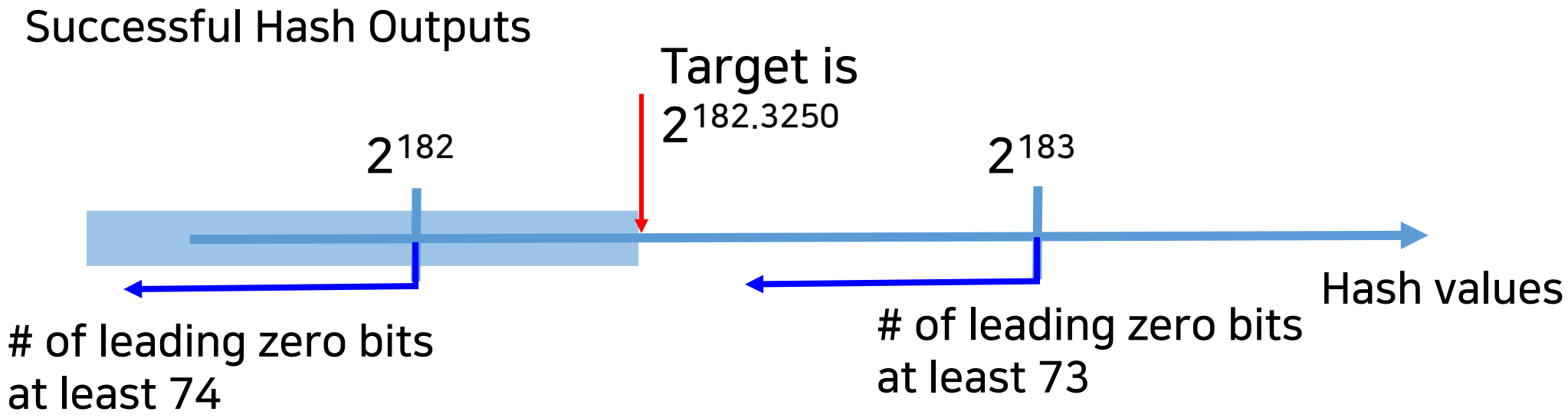
Nonce 1225863608

Bitcoin Difficulty

- Example of Difficulty and Target
  - Block #516445
  - BlockHash 0000 0000 0000 0000 0047 5801 … … … 832b
    - 18 hex zeros * 4 bits/hex + 1 bit = 72 + 1 = 73 bit zeros
  - Difficulty D is 3,511,060,552,899.7197 = 3.5e12
  - Target is $Target_0$ * (1/Difficulty)
    - Log2(D) = 41.68
    - Target = $2^{224.000}$ $2^{-41.675}$
      = $2^{182.325}$

Bitcoin Difficulty

Recall PoW Success
is
SHA Hash Output < Target



Bitcoin Difficulty

- Network Hash Rate : Block#516445
- With D=3.5e12, the probability p is about $2^{-(32+41.675)} = 2^{-73.6750}$.
- Then, it would take $1/p = 2^{73.6750} \sim$ 1.5080 e22 hashes to mine a single block.
- Dividing it by 10 min = 600 sec, the network hash rate is obtained, 25.13 Exa hash/sec.

Exa = 10^{18}

10% 해쉬 파워를 위해 투자해야 할 돈은?

Ex

- Antminer S9s (14 Thps) 이 몇 개 필요할까, 만약 내가 hash power를 0.01 % 갖기를 원한다면?
- 네트워크 hash rate 은 25 Exa hash/sec 이다.

  - You need to bring at least 179 AS9 chips.

$$\text{Your Hash Rate} \geq \frac{0.01\% \;\; \text{Network Hash Rate}}{100\% - 0.01\%}$$

$$= \frac{1}{9999} 25e18 = 25e14$$

$$= 178.6(14e12)$$

- 179000개
- 단가 3000 USD
- 537 MUSD

문제

네트워크 hash rate은 25 Exa hash/sec 이다.

- 현재 네트워크에서 작동하는 마이닝 노드의 최소 개수는 몇 개인가?

답

네트워크 hash rate은 25 Exa hash/sec 이다.

- 현재 네트워크에서 작동하는 마이닝 노드의 최소 개수는 몇 개인가?

$$\text{최소갯수} = \frac{\text{Net HR}}{\text{가장빠른칩 HR}}$$

$$= \frac{25 \times 10^{18}}{14 \times 10^{12}}$$

$$\sim 1.8 \times 10^{6}$$

문제

네트워크 hash rate은 25 Exa hash/sec 이다.

- 한개의 가장 빠른 마이닝칩으로 하나의 블록 작업증명에 성공하려면 걸리는 시간은?

문제

네트워크 hash rate은 25 Exa hash/sec 이다.

- 한개의 가장 빠른 마이닝칩으로 하나의 블록 작업증명에 성공하려면 걸리는 시간은?

$$\text{시간} = \frac{\text{Net HR} \times 600\text{초}}{\text{가장빠른칩 HR}}$$

$$= \frac{25 \times 10^{18}}{14 \times 10^{12}} \times 600\text{초}$$

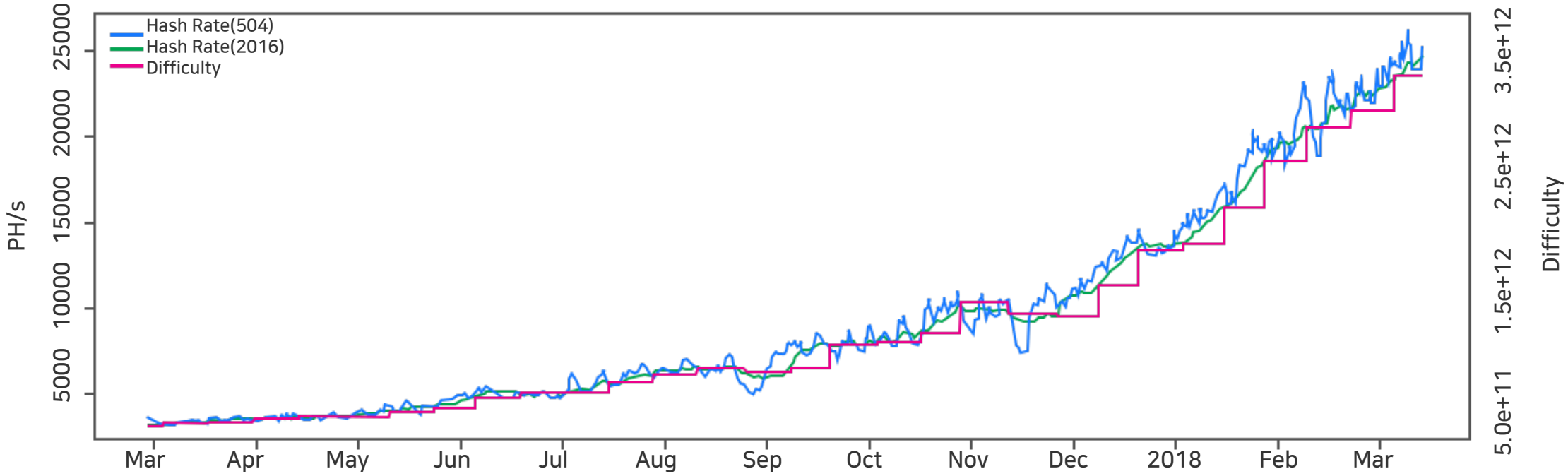
$$\sim 1.07 \times 10^{9}\text{초}$$

$$= 31.7 \text{ 년}$$

일년 = 3153만6천 초

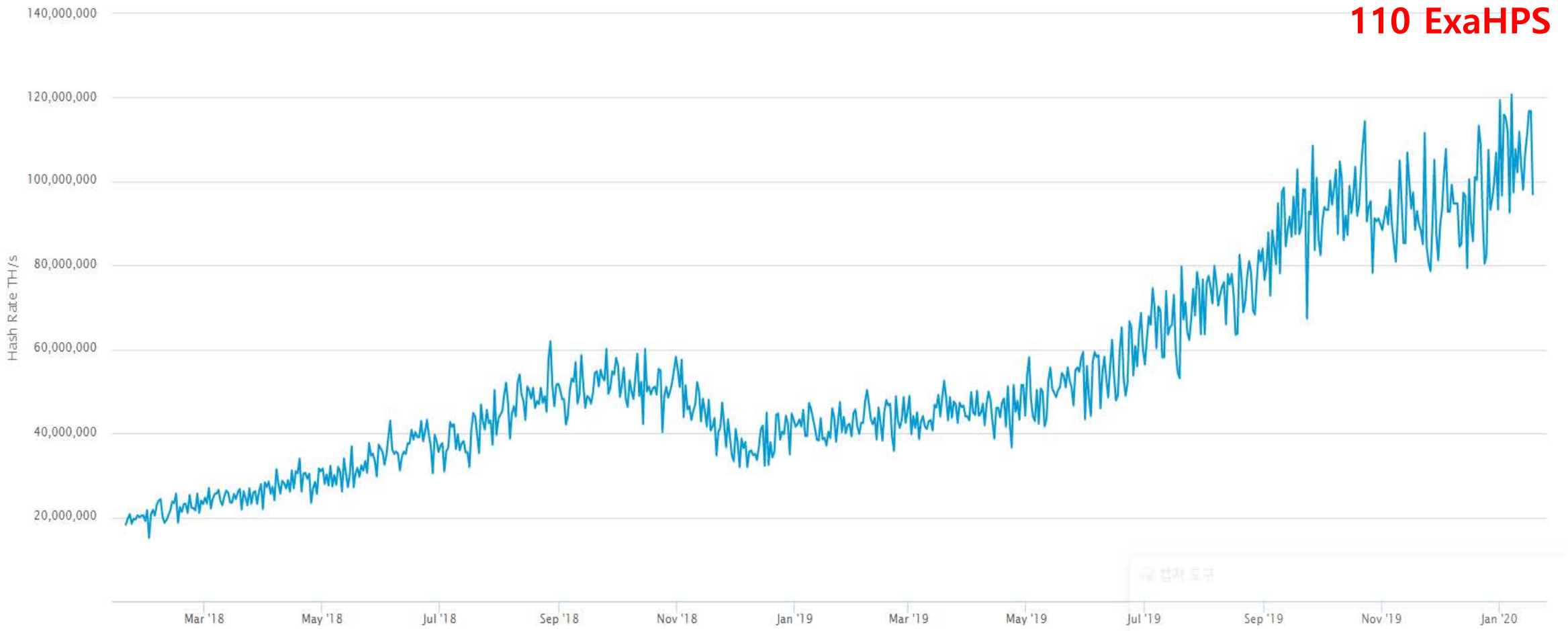
2 History of Bitcoin difficulty

- Bitcoin Hash Rate vs Difficulty (Mar/17 ~ Apr 18)



출처: https://bitcoinwisdom.com/bitcoin/difficulty

Network Hash Rate = 1/p



Goodness of Bitcoin PoW

- PoW provides flexibility in TPS solutions!
  - Small difficulty → fast TPS
  - Large difficulty → slow TPS

- PoW is sufficient for data immutability!

- PoW and blockchain is a technological breakthrough.

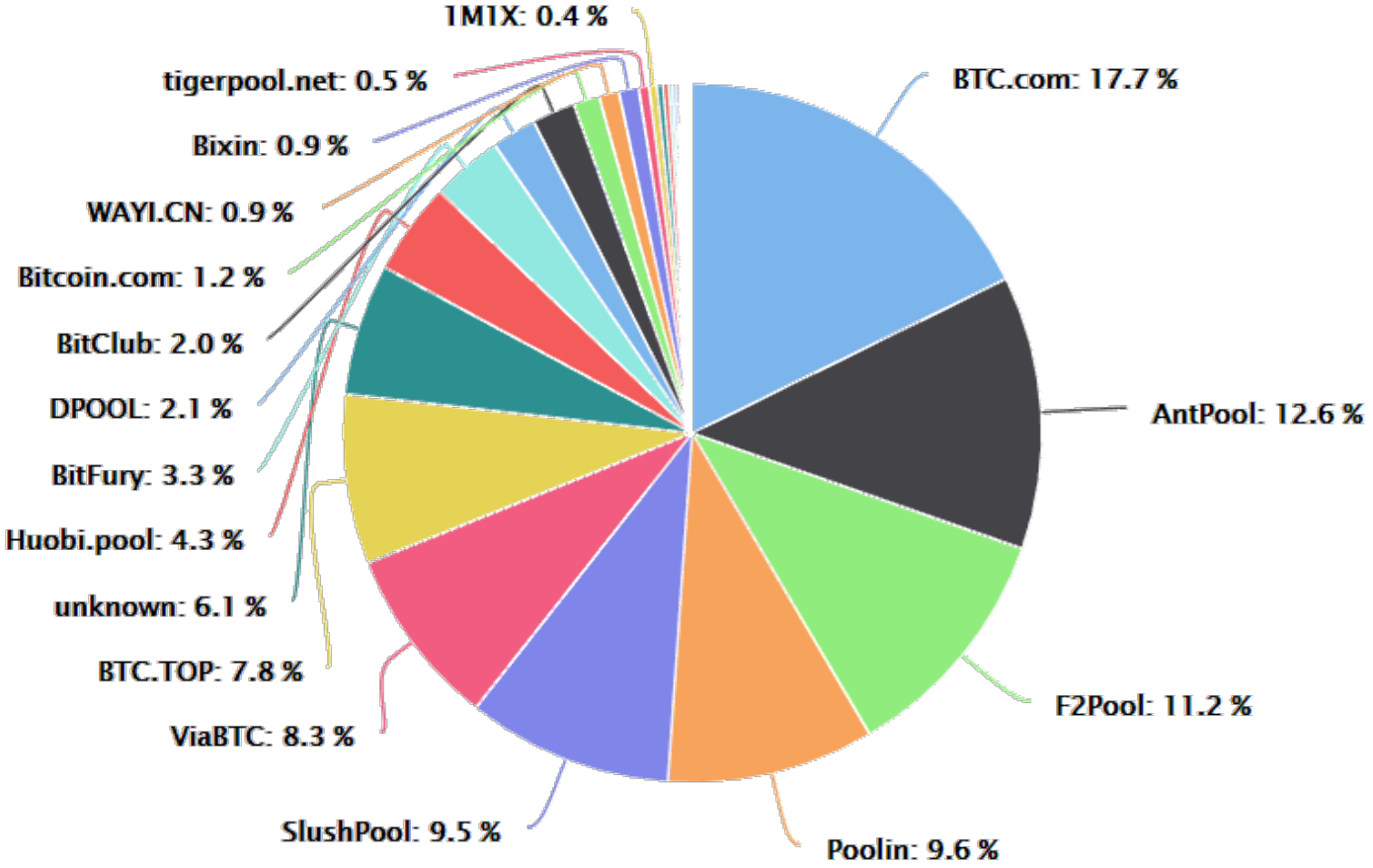
현재 PoW의 문제점

Proof of Work-the Monopoly Problem

- Miners are rational profit seekers.
- They strive to make as much profit as possible.
- Mining operations are highly parallelizable, GPU mining quickly replaced CPU mining:
- FPGAs did GPUs.
- ASICs did FPGAs.

3 Proof of Work-the Monopoly Problem

- Proof of Work, any alternative?
  - PoW, monopolized today.
  - Handful of mining sites dominating.
  - The trust has been degraded.
  - No more one CPU one vote.
  - Rational profit seeking miners use ASICs now.
  - Huge energy spending



https://btc.com/ (기간: 2018. 09 ~ 2019. 09)

Proof of X Schemes

- Proof of Stake (PoS)
- Delegated PoS (DPoS)
- Proof of Activity (PoA)
- Byzantine Fault Tolerant (BFT)

Proof of X Schemes

- Proof of Stake (PoS)
  - Give higher PoW chance to a node with a higher stake (more coins).
  - Good: No high energy consumption
  - Bad: Rich gets richer problem
  - What if the node stays off line?
  - Centralized.
- Delegated PoS
  - Lend coin and share profit.
  - Small number of nodes, off-chain politics

Reference: See page 2114, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

Proof of X Schemes

- Proof of Stake based on Coin Age
  - *Coin age* is no. coins times the holding period.
    - Implemented in Peercoin (peercoin.net).
  - The difficulty of PoW is individually determined, inversely proportional to one's *coin age*.
  - If one finds a solution, one's *coin age* is reset.
  - Slowly increasing the chances of solving the puzzle next time.

Reference: See page 2114, IEEE COMMUNICATIONS SURVEYS & TUTORIALS, VOL. 18, NO. 3, THIRD QUARTER 2016

Proof of X Schemes

- Proof of Stake
  - In contrast to PoW, where the longest block chain survives, *coin age* PoS declares the block chain with the highest total sum of *destroyed coin age* as the main chain.
  - An attacker must hold a huge amount of coins.

Proof of X Schemes

- Proof of Stake
  - Good: Energy consumption is minimized.

[229] N. Houy, “It will cost you nothing to ‘kill’ a proof-of-stake cryptocurrency,” Econ. Bull., vol. 34, no. 2, pp. 1038–1044, 2014.

Proof of X Schemes

- Proof of Stake
  - Bad
    - Coin age accumulates even when the node is not connected to the network.
    - Come online for reward go offline afterwards.
    - The lacking of sufficient number of online nodes, may facilitate attacks.

5 Summary of Altcoins

- Table IV – Summary of Altcoins and Extensions

	Approach	Distinct Feature (incl. References)	Sec.
Precursor	B-Money	Mining reward proportional to proof of work difficulty; requires a broadcast channel [7]	II-B, V-D, V-E
	Bit Gold	Chained proof of work [10]; Byzantine-resilient quorum [13]	III-B, V-D, V-E
	Karma	Distributed currency maintained by a bank set [8]	V-E
	RPOW	Centralized (reusable) proof of work exchange/ bank [9]	V-E
Altcoins	Bitshares (BTS)	Delegated proof of stake [231]	V-F
	Bytecoin (BCN)	Implements CryptoNote [190], which aims for unlinkable and untraceable transactions	V-C, V-E
	Counterparty (XCP)	Colored coin; used proof of burn	V-H, V-H
	Cryptonite (XCN)	Implements the mini block chain scheme [127]	IV-D
	Dash (DASH)	Formerly known as Darkcoin; implements native CoinJoin-like transactions [178]	V-C
	Dogecoin (DOGE)	Block payload holds TXIDs only; fast block generation	IV-D, V-E
	Litecoin (LTC)	Uses scrypt [214] to foster distributed power among miners	V-E
	Mastercoin (MSC)	Colored coin; exodus address	V-H
	Nextcoin (NXT)	Entirely proof of stake based	V-F
	Peercoin (PPC)	Identified coin age as alternative measure; proof of stake [227]	V-F
	Primecoin (XPM)	Proof of work with intrinsic value i. e. prime chains [218]	V-E
	Reddcoin (RDD)	Proof of stake velocity [234]	V-E
	RSCoin	Centrally controlled money supply with distributed verification [126]	IV-D
	Ripple (XRP)	Implements a novel Byzantine agreement protocol [200]	V-D
	Zerocash	Full-fledged altcoin, carrying on the ideas of Zerocoin [189]	V-C

5 Summary of Altcoins

- Table IV – Summary of Altcoins and Extensions

	Approach	Distinct Feature (incl. References)	Sec.
Altchains	Bitmessage	Secure messaging service [145]	IV-G
	Ethereum (Ether)	Turing complete smart contract processing [44], [45]	II-E
	Namecoin (NMC)	Key-value storage; realizes decentralized domain name coordination [143]	IV-G
	Permacoin	Decentralized file storage; proposes proof of retrievability [100]	V-E
Protocols / Extensions	CoinJoin	Uses multi-signature transactions to enhance privacy [160]	V-C
	CoinShuffle	Decentralized protocol to coordinate CoinJoin transactions [180]	V-C
	CoinSwap	Enables P2P-based trustless mixing [41]	V-C
	CommitCoin	Secure timestamping protocol [40]	V-H
	Mini block chain	Identifies individual block chain components [127]	IV-D
	Mixcoin	Mixing with accountability [174]	V-C
	Zerocoin	Unlinkable and untraceable transactions by employing zero knowledge proofs [187]	V-C

CoinMarketCap

Accessed on 1/21/2020

	#	Name	Market Cap
PoW	1	Bitcoin	$157,523,327,976
PoW+PoS	2	Ethereum	$18,237,664,973
BFT	3	XRP	$10,173,030,507
PoW	4	Bitcoin Cash	$6,324,111,387
PoW	5	Bitcoin SV	$5,514,168,411
PoS	6	Tether	$4,642,239,400
PoW	7	Litecoin	$3,703,645,030
DPoS	8	EOS	$3,489,493,081
BFT+PoS	9	Binance Coin	$2,703,188,581
BFT	10	Stellar	$1,257,162,885
PoS	11	Cardano	$1,133,667,715
PoW	12	Monero	$1,132,339,953
DPoS	13	TRON	$1,110,529,913
PoS	14	Tezos	$1,049,197,574
PoW	15	Ethereum Classic	$1,033,632,329
PoW+PoS	16	Dash	$1,025,878,916
	17	Chainlink	$942,976,348
PoW	18	UNUS SED LEO	$888,524,224
BFTPoS	19	Cosmos	$867,402,795
dBFT	20	Neo	$793,931,677

Proof-of-XXX, Alternatives to PoW

	Pros	Cons	Coins within top 50 rank
PoW (Proof-of-Work)	▪ Strongest security ▪ Difficult to produce ▪ Easy to verify	▪ Extreme computing power ▪ 51% attacks ▪ Transaction speed / Transaction throughput	Bitcoin, Ethereum
PoS (Proof-of-Stake)	▪ Energy & hardware efficiency ▪ Expensive 51% attacks	▪ Recentralization ▪ The rich-get-richer ▪ "Nothing at stake" problem	ETH2.0, Cardano, Tezos
DPoS (Delegated PoS)	▪ Scalability and speed ▪ Energy & hardware efficiency ▪ Encouraging good behavior by real-time voting	▪ Recentralization ▪ DDoS attacks	EOS, TRON, NEO
BFT	▪ Resistant to n/3 attacks ▪ Validators are randomly selected.	▪ $O(n^2)$ complexity	XRP, NEO, BinanceCoin, Cosmos

Libra

- 합의알고리즘: **Byzantine Fault Tolerance** O(n^2) + 지분증명
- 노드수 100개
- 1000 ~1500 TPS
- 중앙화 솔루션
- Stable Coin ~ Reserve
- Facebook network has 2B users.
- The era of digital currency may arrive sooner!

Marcus noted that blockchain technology is inevitable and if the U.S. doesn't lead in building and regulating it, the tech will come from places "out of reach of our national security apparatus," raising the spectre of China

LibraBFT

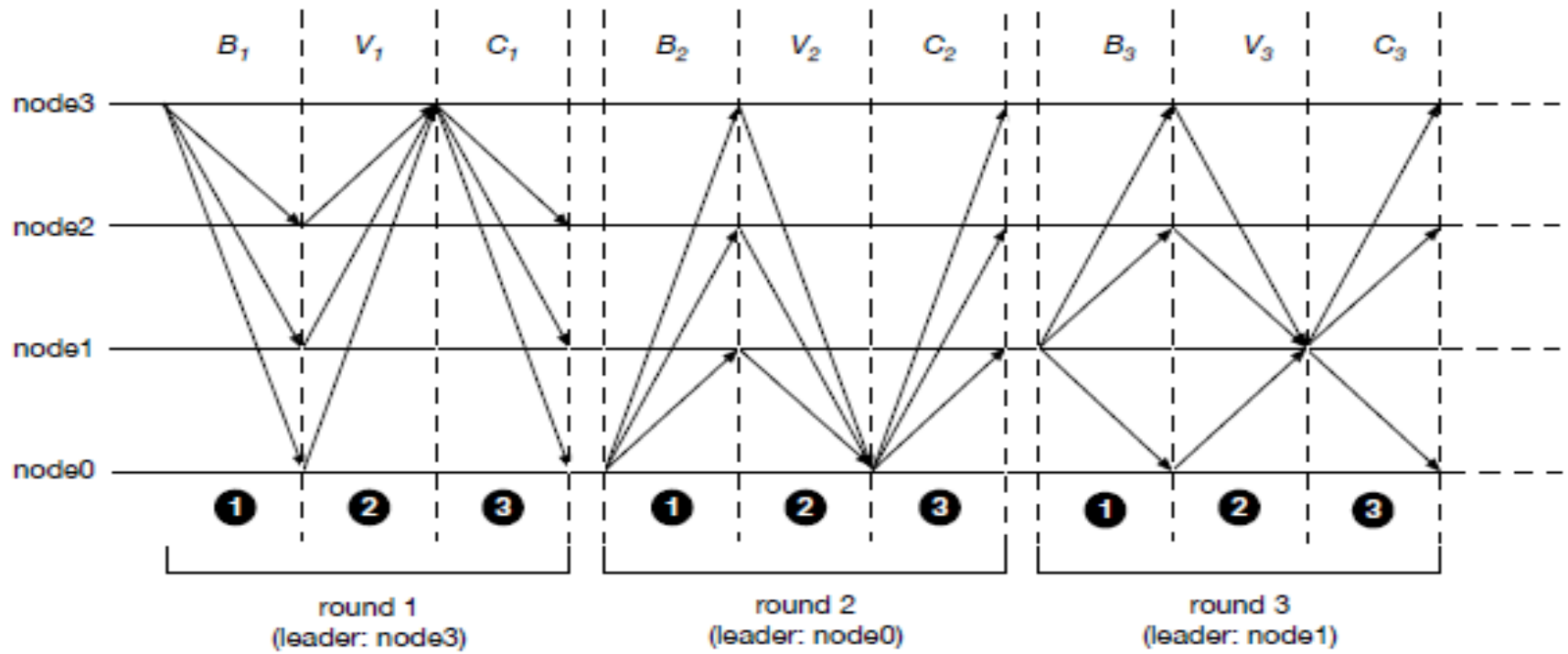


Figure 3: Overview of the LibraBFT protocol (simplified, excluding round synchronization)

PoW는 근본적인 보안성 해결방안

- 탈 중앙성과 보안성 모두 확보 가능한 해결방안!

- 주요 합의알고리즘은 탈 중앙성을 희생하여 보안성과 확장성을 얻으려 목표, 혹은 off-chain 정책에 의존함.
  - Staking, Delegation, Activity-checking, Leader Selecting, Random Selecting, etc.

- PoW의 현재 문제점을 새로운 기술로 해결하면 여전히 가장 좋은 해결방안이 됨!

블록생성과 검증이 분리되면 어떤 일이?

- 랜덤 선출된 자가, 지분을 많이 가진 자가, 활동이 많은 자가, 장군으로 선출된 자가, …

블록을 생성하세요.

- 나머지는 검증을 하겠습니다.
- 선출 → 생성 → 검증 등 여러 단계로 분리 됨.
- 각 단계에서 일이 제대로 되었을까?
  - Validators를 뽑아서 합시다. 보상은 나눕시다.
- 생성자 혹은 검증자가 일을 대충해서 좋지 않은 TX가 들어갈 경우?
  - 각 단계에서 혹시 실패한 경우가 발생할 경우는…
  - 평판도 측정, Staking 압수, …

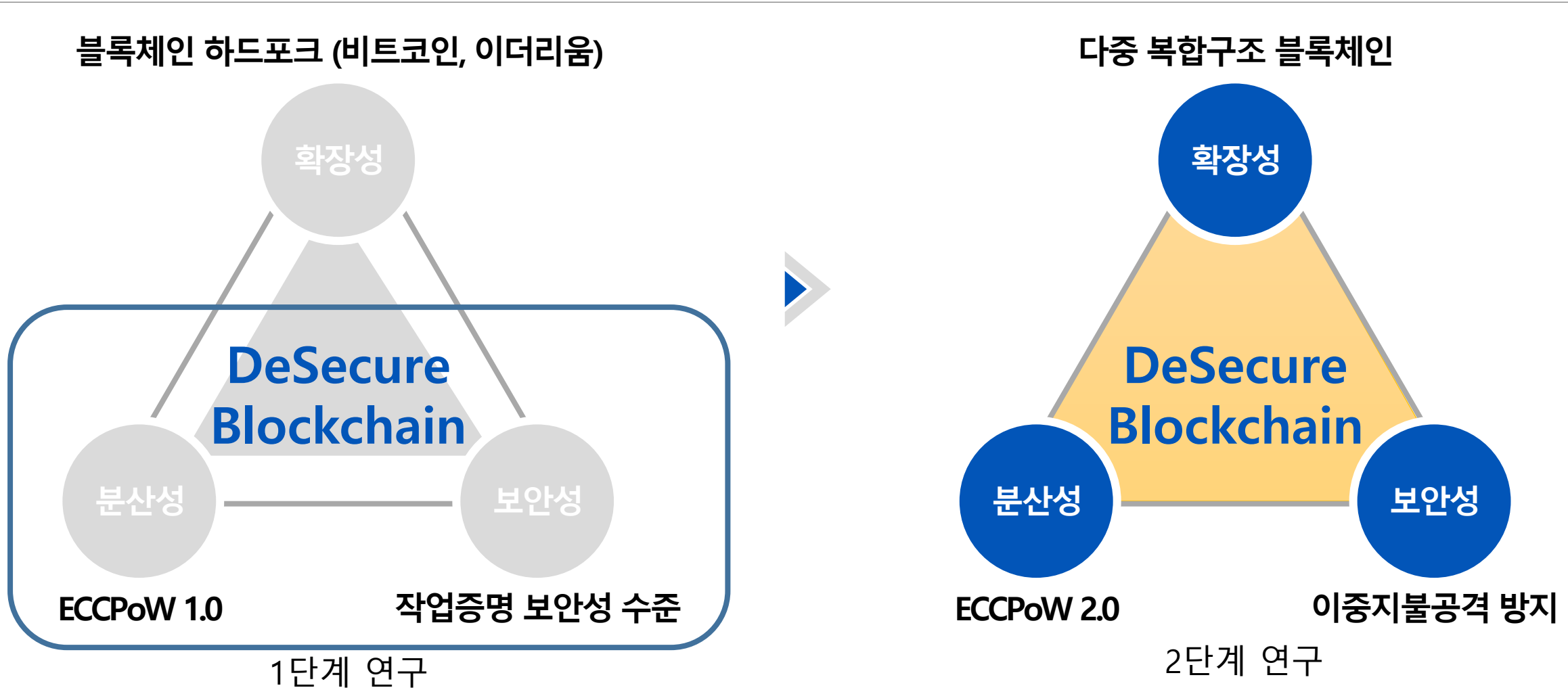
PoW는 생성과 검증이 동시에 이루어짐

- 수 많은 노드가 생성과 검증을 경쟁적으로 (동시에) 함
- 끊김이 없이 블록이 생성됨
- 앞으로 전진만 있음
- 잘못된 TX이 포함될 경우 헛고생, 스스로 검증하고 생성함

블록체인 트릴레마 (V. Buterin)

구분	내용	사례
확장성 (Scalability)	사용자 수 증대에 유연하게 대응할 수 있는 능력 단위 시간당 거래건수가 늘어 날 때 무리 없이 거래를 증대시킬 수 있는 능력을 의미	이더리움 Plasma, Sharding
탈중앙성 (Decentralization)	중앙 집중화 구조를 벗어나 노드들이 소규모 네트워크로 **자율적으로 모여 운영주체가** 되는 것을 말함 기존의 서버-클라이언트 관계를 벗어나 개별 노드들이 자발적이고 자율적으로 피투피(P2P) 방식으로 연결함 블록체인 기술이 사회적으로 널리 확산됨에 따라 **기존의 중앙집중식 조직, 기업, 단체, 기구** 등은 **탈 중앙 구조로** 변경되고 있음	초기 Bitcoin Network
보안성 (security)	블록체인 **데이터의 무결성 확보**하거나, 오픈 프로토콜이 원래 의도한 바 데로 시스템이 작동하도록 하고, 외부로 부터의 공격으로 부터 **시스템을 보호**하는 능력 을 의미	

Research at GIST Blockchain Economy Center

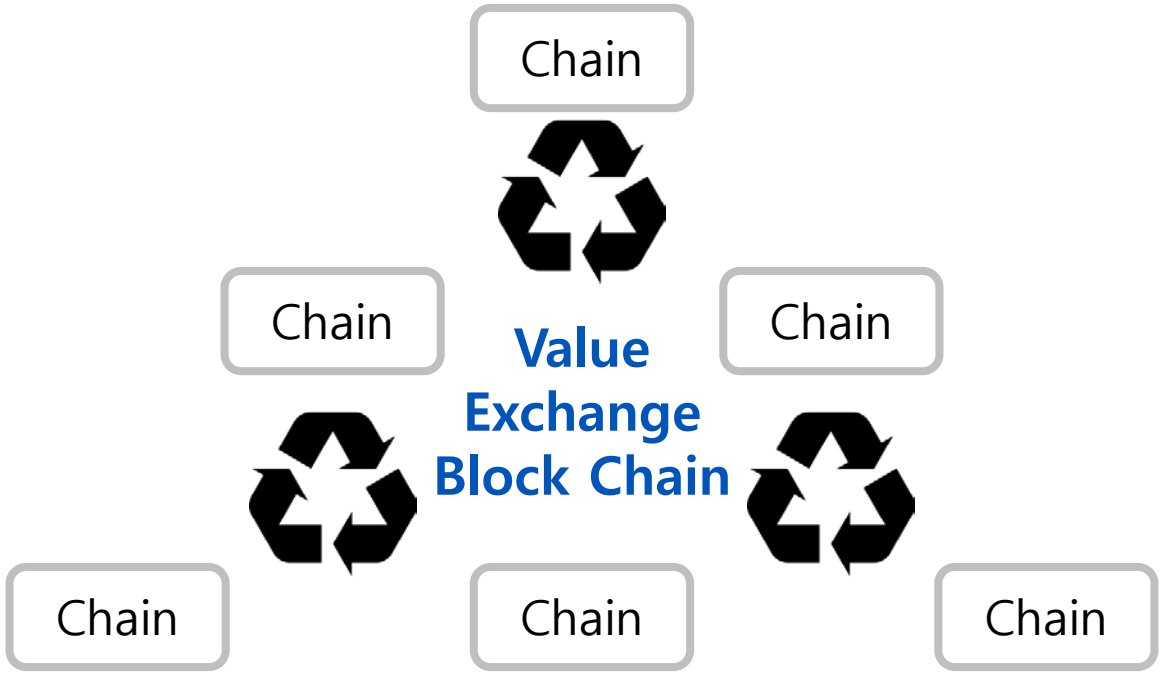


확장성 강화 연구 with DeSecure Blockchains

- Evolutionary Space에서 DeSecure 블록체인을 용도에 따라 특화
- 용도별 특화 블록체인들을 연결하여 다중 복합구조 DeSecure 블록체인 형성

Low TPS
Global Nets
High Delay

Large Tx (Assets)



High TPS
Local Nets
Low Delay

Small Tx
(Utility Coins)

<용도에 따라 세분화된 다중 복합구조 블록체인>

Comparison to Existing Scalability Solutions

DeSecure Blockchain aims to resolve scalability issue with promotion of competition.

Type	DeSecure	Bitcoin		Ethereum	
Name	Multi-level, multiple chains	Seg-Wit	Lightening Network	Plasma	Sharding
How	Many ECCPoW based chains can talk to each other via value-exchange service	Realize by modifying a block data structure	Allow off-chain transactions and record the end result of these transactions into the main blockchain	Allow transactions in child chains, TX records end up at the main chain are limited.	Divide BC DB with multiple shards
Pro	Many different services and levels of chains can co-work.	Easy to realize	Faster transactions Small TX fees	Faster transactions Small TX fees	Faster transaction
Con	No single chain solution Requires an ecosystem	Small improvement	The content of off-chain transactions lost	Some TX content lost Only full node can run this	Increased SW complexity

블록인터벌을 10분에서 1분으로 줄이려면 어떻게 될까?

블록인터벌을 10분에서 1분으로 줄이려면 어떻게 될까?

수 많은 fork가 매 번 발생하는 문제 발생, 비 동기화
DS 공격 취약성을 따져봐야
그러나, Profitable DS Attack분석으로 해결 가능 (See DeSecure블록체인)
소규모 네트워크, 용도별, 지역별로 쓰는 용도를 다르게 할 수 있다.

네트워크 별, 용도별, 지역별 로 서로 다른 블록체인 만들고 연동 시킨다!

이 것을 가능하게 하는 필요 조건은 무엇인가?

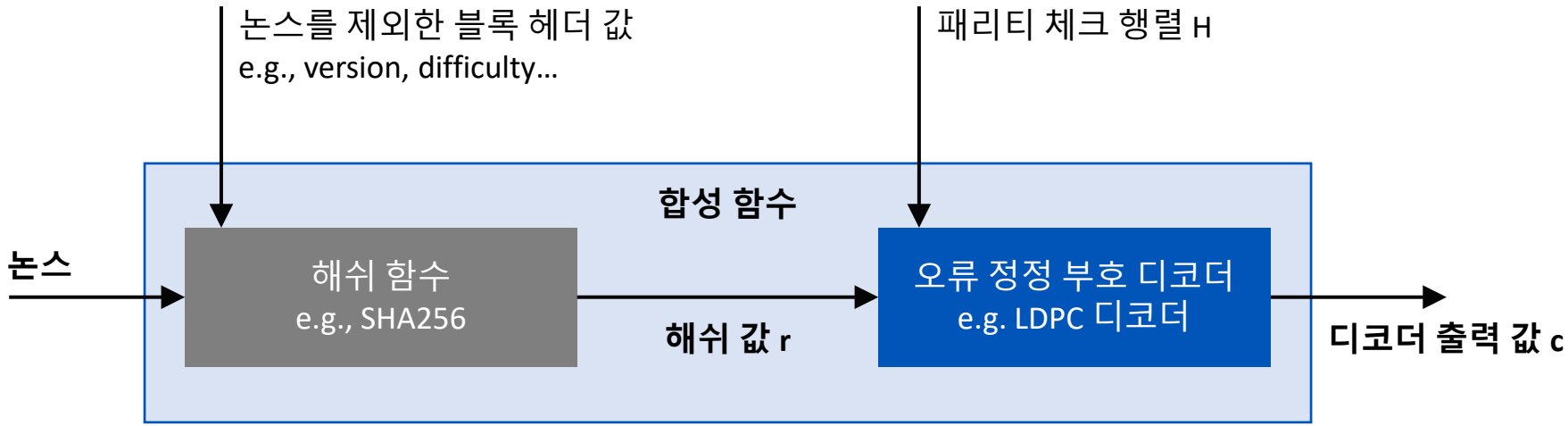
Key New Idea is a TV Puzzle System!

- 새로운 PoW 알고리즘 개발을 위해 고려해야 할 사항
  - Puzzles 문제를 다양화 하고, 문제 출제 방식을 시시각각 바꿀 수 있게 한다.

  - A puzzle should be difficult to solve but very easy to check.
  - The puzzle should be resistant to attacks.
  - Solution to the puzzle for a block should not be reusable.
  - Puzzle difficulty should be adjustable.
  - Anyone with a CPU who wishes to participate should be able to join.
  - Consensus must eventually be reached; there must be a common rule to resolve forks and to determine the main blockchain.

부호 – 암호 작업증명

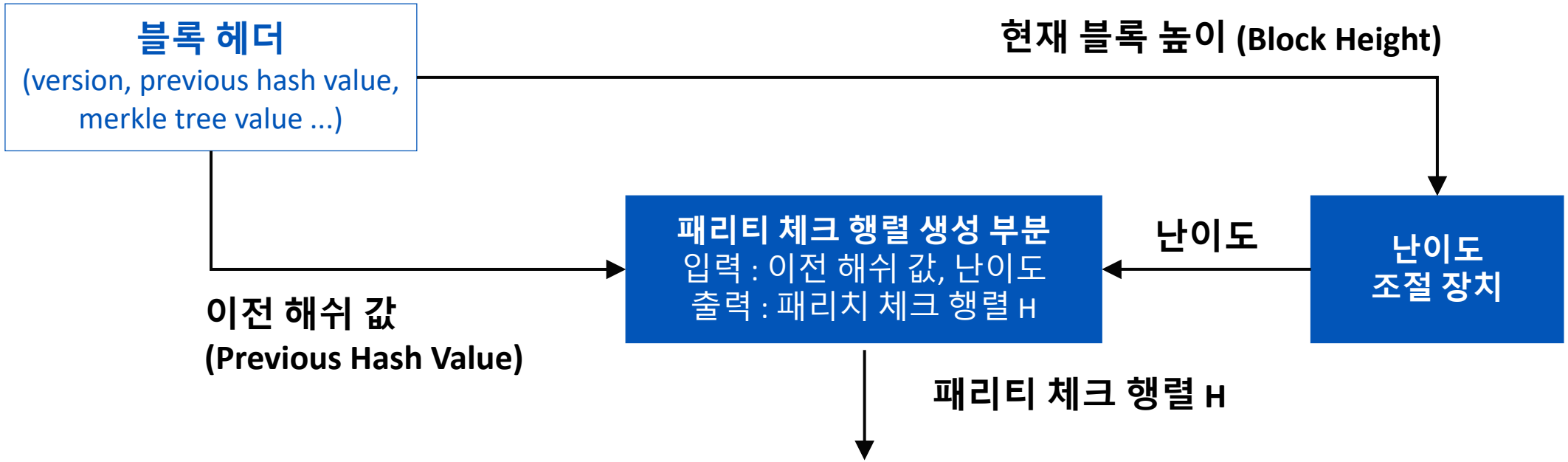
- 부호-암호 작업증명 (ECCPoW) 정의 :
  오류 정정 부호와 작업증명을 동시에 사용하여 분산성/보안성을 확보하기 위해 개발된 작업증명 기술임.
- ECCPoW은 매 블록마다 변하는 합성 함수를 사용함.



- (**시변성**) 패리티 체크 행렬을 매 블록 마다 변경함으로써, 함성 함수를 매 블록 마다 변경 할 수 있음.
- (**무한성**) 무한히 많은 패리티 체크 행렬을 사용하면, 무한히 많은 합성 함수를 생성 할 수 있음.

매 블록마다 바뀌는 암호 퍼즐 생성 (1)

- 난이도는 "블록 길이" 및 "부호의 비율"을 결정
- 이전 해쉬 값을 이용해 Gallager code 생성 방법의 순열 순서를 결정



Time-Variant Proof-of-Work Using Error-Correction Codes

Sangjun Park, Haeung Choi, and Heung-No Lee, *Senior Member, IEEE*

***Abstract*— The protocol for cryptocurrencies can be divided into three parts, namely consensus, wallet, and networking overlay. The aim of this consensus part is to deal with coming to an agreement among nodes to the current status of their blockchain. This status must be updated only through valid transactions and it is achieved among trustless rational peer nodes. A proof-of-work (PoW) based consensus has been proven to be secure and robust owing to its simple rule and has served as a firm foundation for cryptocurrencies such as bitcoin and ethereum. However, the usage of specialized mining devices for the existing PoWs causes two problems: *i*) the re-centralization issue of a mining market and *ii*) the usage of a considerable amount of energy in mining. In this paper, we propose a new PoW called Error-Correction Codes PoW (ECCPoW) where the error-correction codes and their decoder can be utilized by concatenating the decoder with a hash function. In ECCPoW, puzzles can be intentionally generated to vary from block to block, leading to a time-variant property. This property is useful in repressing the emergence of the specialized mining devices, which can be a solution to the problems that the existing PoWs face currently with**

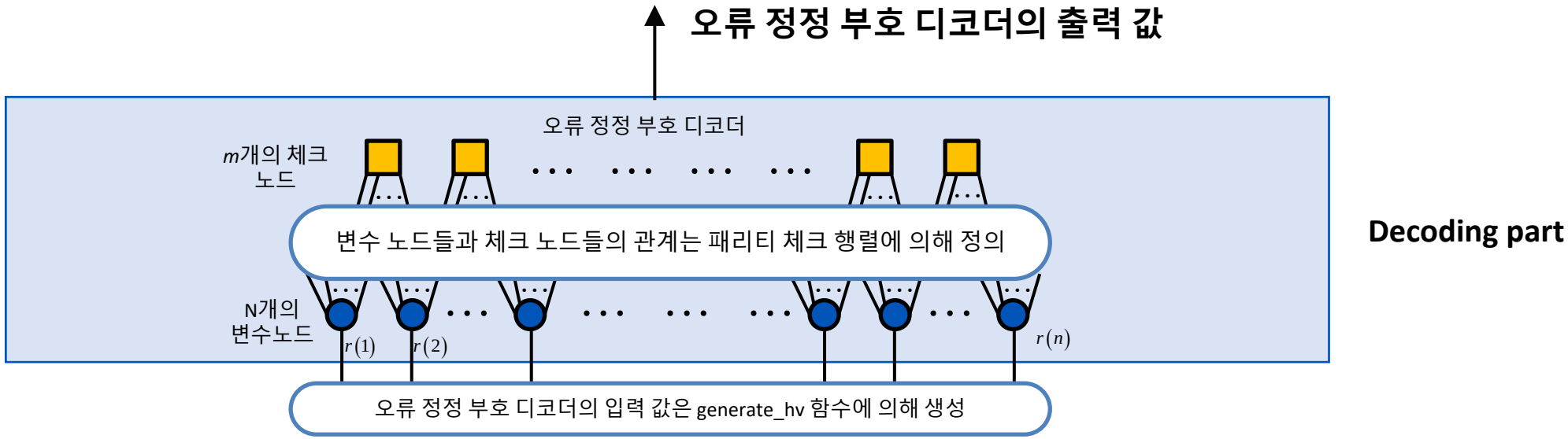
***Index Terms*— Consensus, Cryptocurrency, Blockchain, Proof-of-Work, Error-Correction Codes, Hash Functions**

blocks can be possible In contrast, if PoW is attached to each mined block, attackers cannot make any unauthorized modifications without redoing all the works. No one thus can alter any mined blocks, meaning an immutability property.

In bitcoin, miners make rational decisions to maximize their profits. These decisions are conducted by following two stages. First, the miners select a blockchain in which its height is the longest. Second, they extend this longest one by adding a newly mined block which is a result of solving a puzzle generated in PoW. To evaluate the quality of the decisions, we consider an example. At a certain time point, suppose there are two chains in which one chain is longer than the other chain. The longer chain shall be treated preferable and more trustable because it has the more PoW accumulated, meaning that it is more difficult to alter. Thus, miners shall select and extend the longer chain. Making such a selection is good for keeping the mining rewards. The mining reward is actually a delayed conditional payment. Given the miner who mined a certain block at a certain time point t_1, the decision to execute the reward is delayed only after a certain amount of time has passed since the time point t_1. This holding time is measured in terms of number of

매 블록마다 바뀌는 암호 퍼즐 디코더 개발 (2)

- 오류 정정 부호 디코더 입력 값 생성

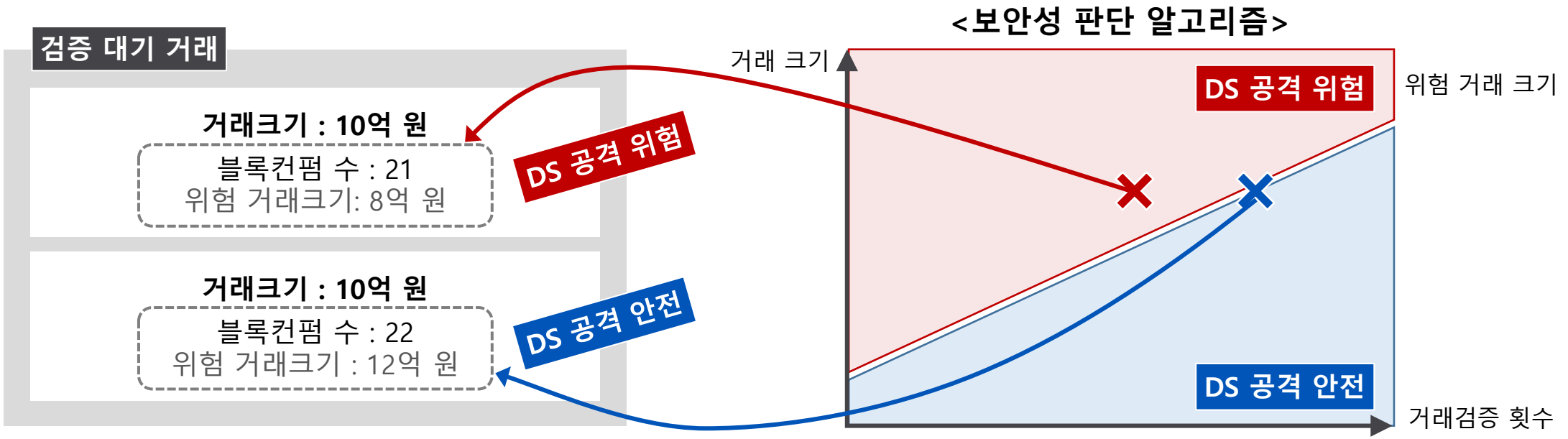


- 패리티 체크 행렬의 변경은 변수/체크 노드들의 관계의 변경을 야기함.
- 즉, 동일한 입력 값을 취득하더라도, 패리티 체크 행렬이 변경되면 상이한 값을 산출함.
- 디코딩은 메시지 전달 알고리즘에 의해 이뤄짐.

보안성 강화 연구

TX Size별로 보안성을 판단해 각자 대처

- 거래 별로 DS공격의 위험성을 평가하여 사용자가 보안위험 자각 및 대처 가능
- 거래검증 횟수와 거래크기가 DS 공격자에게 이윤을 발생시키는지를 거래 별로 평가 가능



Scalable DeSecure Blockchain 개발/보급

- 부호-암호 화폐 시스템 (GIST특허 2018)
  - Error-Correction Code 기반 PoW
  - 재-중앙화 문제 해결 (SHA함수에 전적으로 의존 ASIC칩)
  - 누구나 화폐 발행에 참여 가능

- 세월의 검증을 이겨낸 Bitcoin과 Ethereum의 합의알고리즘에 적용, 보급, 확산 계획

- 탈 중앙적이며 안정적인 Bitcoin과 Ethereum 보급
  - Scalability 문제 해결

ECCPoW resolves the issue of Recentralization!
[See Ref 1]

- Uses time-variant Error-Correction Code(ECC) PoW
  - ASIC/FPGA/Pool resistant
- Achieves a decent decentralization
  - People with a cpu or a gpu can participate!
- Provides energy efficient operation
  - Small hash power needed: O(10^10), instead of O(10^20)
- Offers ECCPoW puzzles completely different from SHA-PoW
  - There are many mining chips available for SHA-PoWs.
  - They cannot be utilized to launch a DS attack to ECCPoW.

Aim to launch BTC-ECC first.

LiberVance

- BTC-ECC hardfork has been 90% completed.
- Raise funding with BTC-ECC.
- Pressing to launch BTC-ECC in 2nd Qtr 2020.

- Fund raised from BTC-ECC will be used to help a series of follow-up projects.

Today money is not honest!

[Hayek has predicted in Denationalization of Money]

- P.24. Free trade in money. As soon as the public became familiar with the new possibilities, any deviations from the straight path of providing an honest money would at once lead to the rapi d displacement of the offending currency by others.
- P. 115. There is no better case for preventing the decrease of the quantity of money circulating in a region or sector of a larger community than there is for governmental measures to preven t a decrease of the money incomes of particular individuals or groups—even though such mea sures might temporarily relieve the hardships of the groups living there. It iseven essential for honest government that nobody should have the power of relieving groups from the necessity of having to adapt themselves to unforeseen changes, because, if government can do so, it wil l be forced by political necessity to do so all the time.
- P. 116. Such areas in which one currency predominates would however not have sharp or fixed boundaries but would largely overlap, and their dividing lines would fluctuate. But once the pri nciple were generally accepted in the economically leading countries, it would probably spread rapidly to wherever people could choose their institutions. No doubt there would remain encla ves under dictators who did not wish to let go their power over money—even after the absenc e of exchange control had become the mark of a civilized and honest country.

The Hayek's Proposal

- The concrete proposal for the near future, and the occasion for the examination of a much more far-reaching scheme, is that
- the countries of the Common Market, preferably with the neutral countries of Europe (and possibly later the countries of North America) mutually bind themselves by formal treaty not to place any obstacles in the way of the free dealing throughout their territories in one another's currencies (including gold coins) or of a similar free exercise of the banking business by any institution legally established in any of their territories.

Which sort of currency would the public select? [Hayek pg 66]

- Four uses of money
  - (i) Cash purchases
  - (ii) Saving
  - (iii) Standard of deferred payments
  - (iv) A reliable unit of account

Hayek argues that money is a commodity that would be better off supplied through competition.

- Monopoly of government vs. competition by private issuers.
- The advantages of competitive currencies are not only removing the power of government to inflate the money supply but also that they would go a long way to prevent the destabilizing fluctuations that government monopoly of money has precipitated over the last century.
- In addition, it makes it difficult for government to inflate its own expenditures.
- The central theme is crystal clear: government has failed, must fail, and will continue to fail to supply good money.

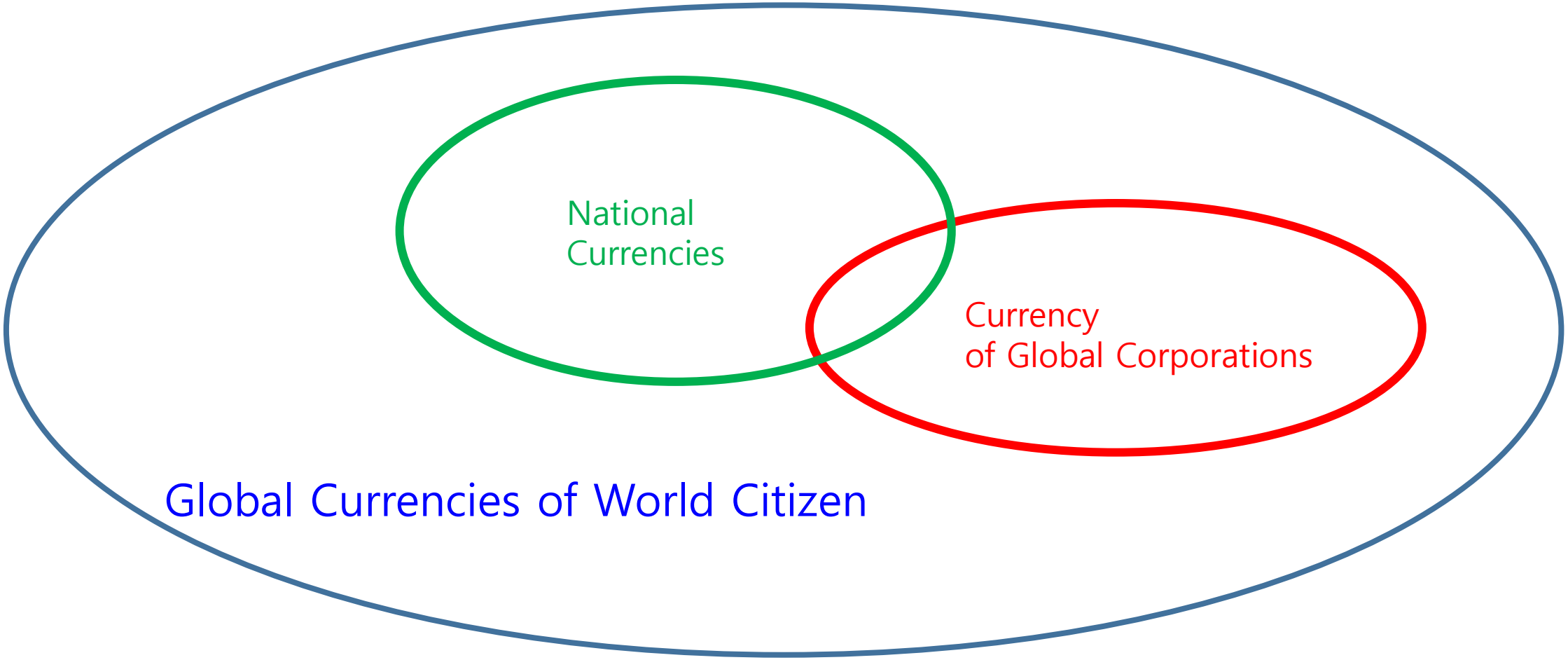
BIT-ECC is money of people!

- We are people from the globe.
- We have our computers shared.
- This computer network maintains the book of transactions.
- This computer network mints coins.
- Currency is created by us the people.
- We the people get the seigniorage.
- Supply of this global currency is fixed.

BIT-ECC provides honest money!

- It is a money freely traded worldwide.
- Supply is fixed.
- Participation is open.
- BIT-ECC is more decentralized than BIT.

10 years from now, competing currencies



Concluding Remarks

- Bitcoin is the currency of world citizen.
- PoW is fundamental to decentralization and security.
- Centralized altcoins are not as valuable as bitcoin.
- DeSecure blockchains and multi-level blockchains provide new technological advance.
- It is inevitable to use cryptocurrencies.

References

1. **Heung-No Lee, "DeSecure Blockchains," ETH-CON, Seoul, Reb. of Korea., May 2019.**
2. **Heung-No Lee, "Blockchain Consensus and Governance," July Meet-Up, Institute of Blockchan and Law, July 11th, 2019. YouTube Video Available at** https://www.youtube.com/watch?v=7ujkFgsKPdY.

Selected References of GIST Blockchain Economy Center

- [Lee1] JH Jang and Heung-No Lee, "Profitable Double Spending Attacks," March 5th, 2019 submitted to IEEE Trans. Information Forensics and Securities, downloadable from https://arxiv.org/abs/1903.01711.
- [Lee2] 장재혁, 이흥노, "50%미만 이중 지불 공격", OSIA S&TR Journal, Vol. 32, No. 1, Mar. 2019. (pdf)
- [Lee3] 정현준, 이흥노, "암호화폐 투자와 규제 현황", 한국정보과학회, 정보과학회지, 제 36권, 제 12호, pp. 49-56, Dec, 2018. (pdf)
- [Lee4] 박상준, 김형성, 이흥노, "Introduction to Error-Correction Codes Proof of Work," 블록체인경제 특집호, 대한전자공학회지, June 2019.
- [Lee5] Sangjun Park, HS Kim, Heung-No Lee, "Time-Variant Proof-of-Work Using Error-Correction Codes," to be submitted to IEEE Trans. Information Forensics and Securities.
- [Lee6] Mohamed Yaseen.J, Giljun Jung and Heung-No Lee."Decentralized Framework for Medical Images Based on Blockchain and Inter Planetary File System", The 41st Annual International Conference of the IEEE Engineering in Medicine and Biology Society(EMBC 2019), Berlin, Germany, Jul. 23-27, 2019.
- [Lee7] Please visit INFONET home page https://infonet.gist.ac.kr/?page_id=14 for more references.