2025.08.14

안효성

채굴의 원리

비트코인 반감기 일시 정리

반감한 개수	날짜	반감 시 블록 높이	반감기 전 블록 보상(블록당 비트코인)	반감기 후 블록 보상(블록당 비트코인)
1	2012-11-27	210,000	50	25
2	2016-07-09	420,000	25	12.5
3	2020-05-11	630,000	12.5	6.25
4	2024-04-20	840,000	6.25	3.125
5	2028-04-17	1,050,000	3.125	1.5625
6	2032	1,260,000	1.5625	0.78125
7	2036	1,470,000	0.78125	0.396025

비트 코인은 4년마다(21만 블록마다) 채굴 보상이 절반으로 줄어듬
-평균 10분당 1개 채굴

https://biz.chosun.com/stock/finance/2024/03/17/QWJPN63RXVECBLICWDMCKA37HA/

비트코인 반감기에 코인 광산 아프리카·남미로 이동

입력 2024-03-24 14:07:40 수정 2024.03.24 17:58:58 실리콘밸리=윤민혁 특파원

비트코인 반감기가 한 달 앞으로 다가온 가운데 '코인 광산'이 에티오피아·파라과이 등 아프리카·남미 국가로 옮겨가고 있다. 반감기가 지나면 비트코인 채굴량은 절반으로 줄어든다. 수익성 감소가 예상되자 미국 등 전기 값이 비싼 지역에서 저렴한 국가로 구형 채굴기가 대량 수출되고 있는 것이다.

중국 코인 채굴 업체 비트메인의 채굴 광산. 사진 제공=비트메인

오늘의 핫

K에너

전국

김건

비트

https://www.sedaily.com/NewsView/2D6REUHRLA

순서

노드 구성

노드를 구성하는 것들

골든 넘버

nonce와 timestamp의 변화=> 해시 변경

체이닝

노드에 연결되는 과정

번외

작업 증명 vs 지분증명

노드 구성

SHA256 해시방법 사용
역해시 불가능

genesis block
연결 리스트 head node 느낌

H

채굴 난이도
로또 번호
merkle root

BH_1

version	(4 bytes)
prev	(32 bytes)
time	(4 bytes)
bits	(4 bytes)
nonce	(4 bytes)
Tx root	(32 bytes)

80 bytes

H

BH_2

prev

Tx root

H

BH_3

prev

Tx root

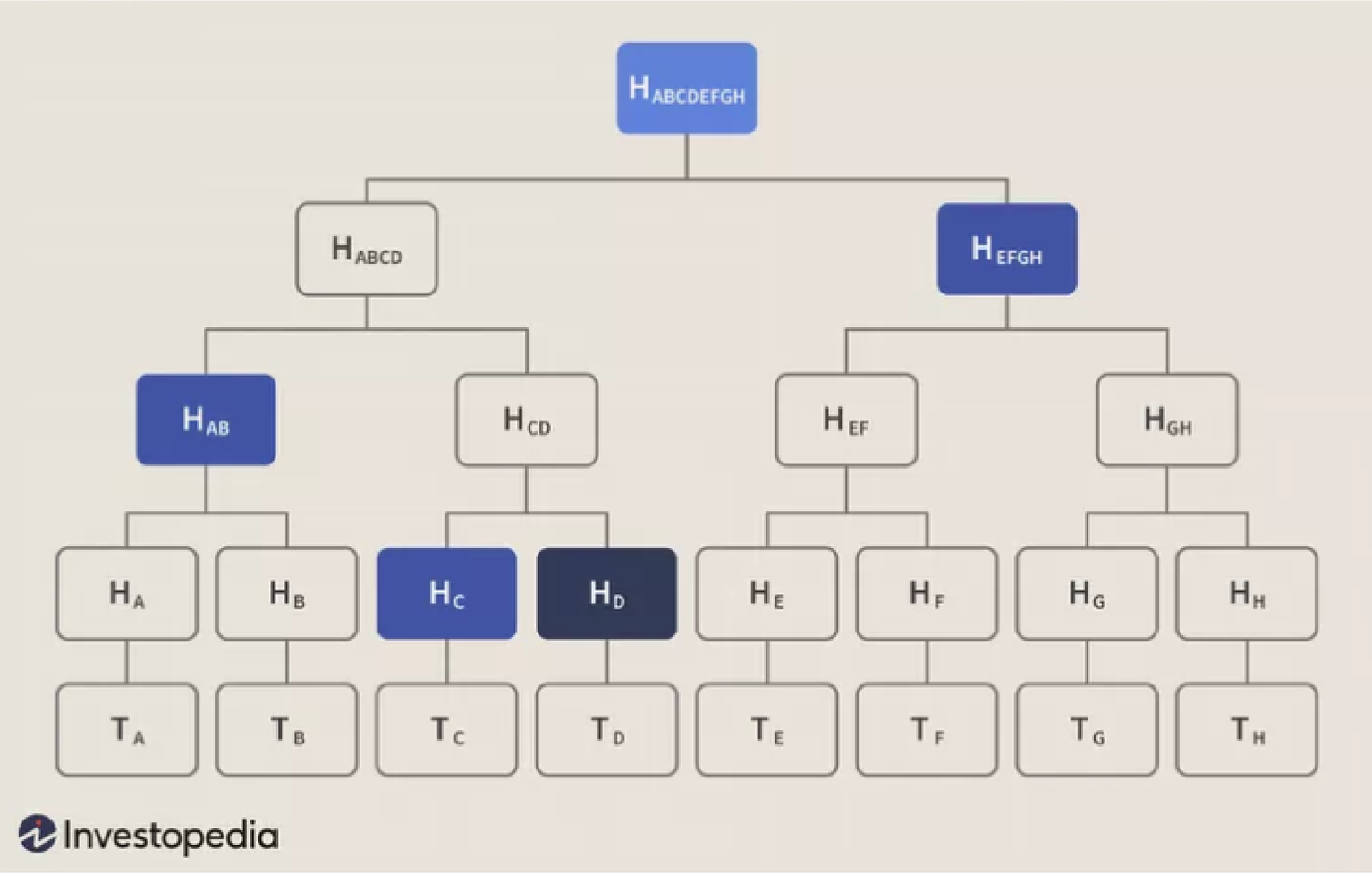
...

coinbase Tx

coinbase Tx

노드 구성

머클 트리



해시에 해시에 해시에 해시...

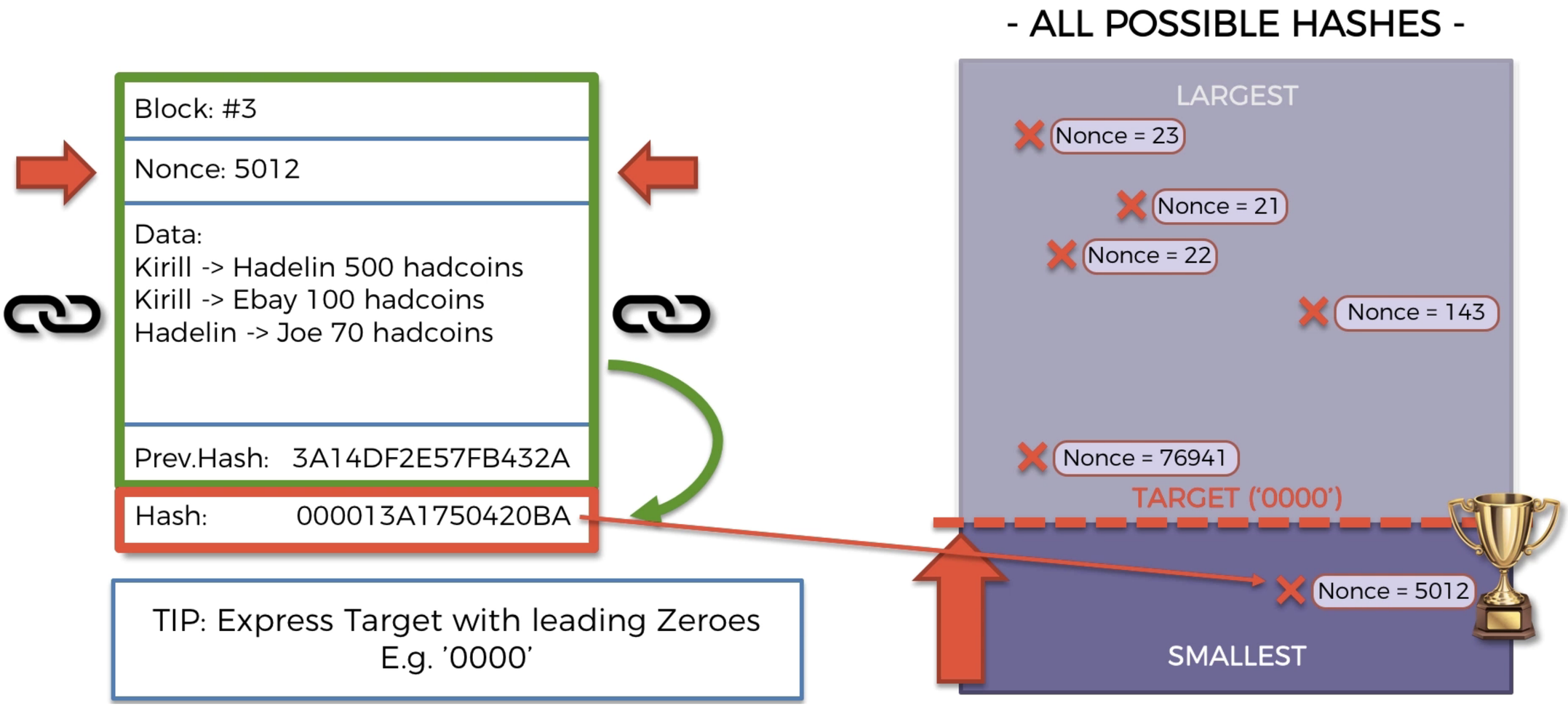
해시 스완..

Tx 정보 압축

노드 구성

Timestamp	2020-09-15 17:25	
Height	648493	노드 번호
Miner	SlushPool	
Number of Transactions	2,826	거래 갯수
Difficulty	17,345,997,805,929.09	채굴 난이도
Merkle root	350cbb917c918774c93e945b960a2b3ac1c8d448c2e67839223bbcf595baff89	
Transaction Volume	11256.14250596 BTC	처리된 거래량
Block Reward	6.25000000 BTC	채굴 보상
Fee Reward	0.89047154 BTC	채굴자가 받는 거래 수수료

채굴


Block: #3
Nonce: 5012
Data:
Kirill -> Hadelin 500 hadcoins
Kirill -> Ebay 100 hadcoins
Hadelin -> Joe 70 hadcoins
Prev.Hash: 3A14DF2E57FB432A
Hash: 000013A1750420BA
TIP: Express Target with leading Zeroes
E.g. '0000'
- ALL POSSIBLE HASHES -
LARGEST
Nonce = 23
Nonce = 21
Nonce = 22
Nonce = 143
Nonce = 76941
TARGET ('0000')
Nonce = 5012
SMALLEST

논스는 4바이트=32비트

0부터 $2^{32} - 1$ (약 42억 9천만)까지의 값을 가짐. 하지만 경우의 수를 담기엔 너무 작다!!!

Let's do some estimations:

Difficulty:

Total possible 64-digit hexadecimal numbers: 16 x 16 x …. x 16 = $16^{64} \approx 10^{77}$

Total valid hashes (with 18 leading zeros): 16 x 16 x … x 16 = $16^{64-18} \approx 2 \times 10^{55}$

Probability that a Randomly picked hash is valid: $2 \times 10^{55} / 10^{77} = 2 \times 10^{-22} = 0.00000000000000000002\%$

Nonce:

The Nonce is a 32-bit number, the Max Nonce = 2^{32} = 4,294,967,296 = 4×10^{9}

Assuming no collisions, this means 4×10^{9} different hashes

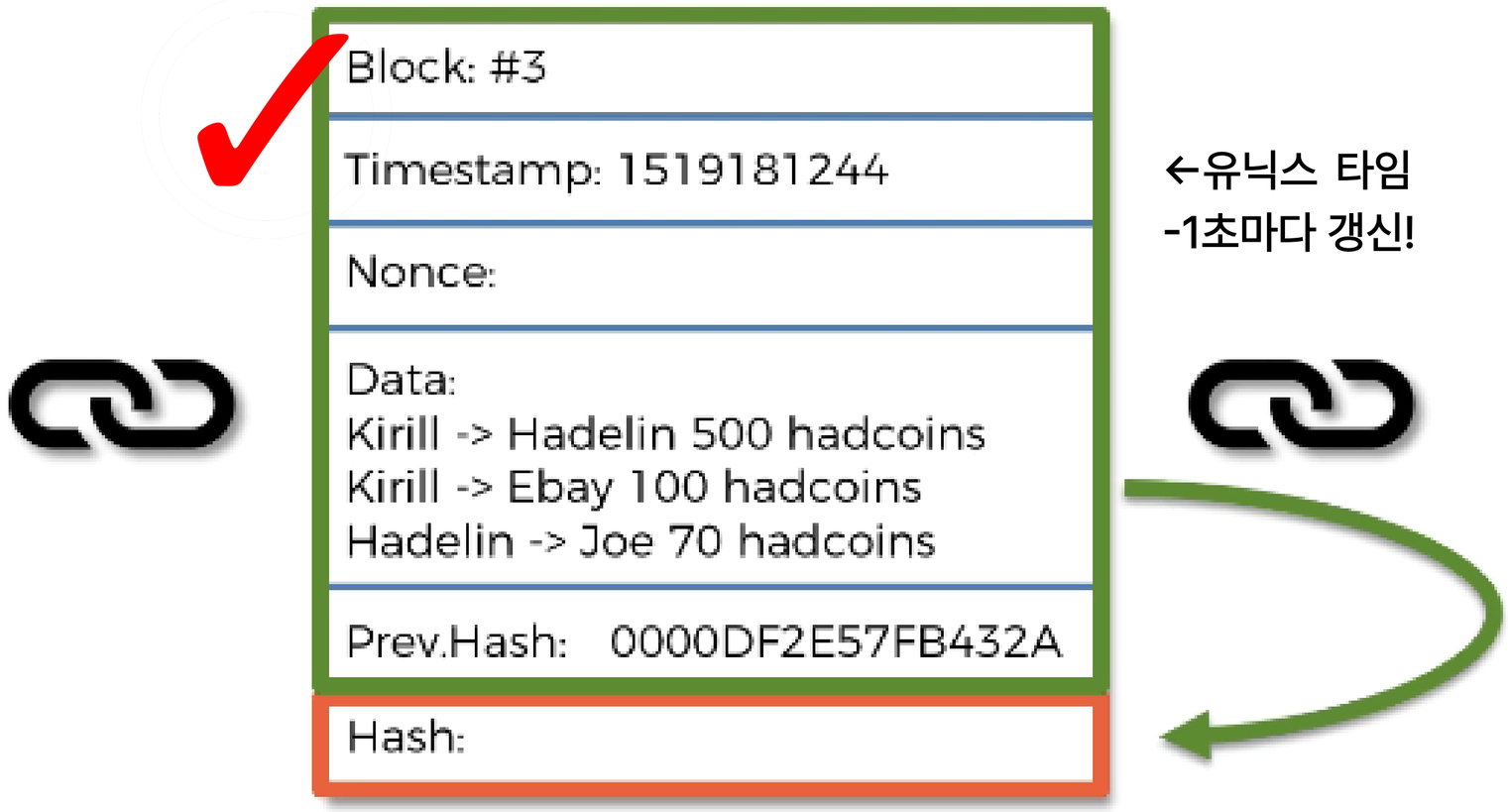
Probability that ONE of them will be valid: $4 \times 10^{9} \times 2 \times 10^{-22} = 8 \times 10^{-13} \approx 10^{-12} = 0.0000000001\%$

Conclusion: One Nonce Range is not enough

초당 1억 연산을 하는 채굴기가 있다고 가정(가장 느린것도 가장 빠른 것도 아님)

그럼 40초만에 40억 연산이 끝나버리는데...??!

채굴



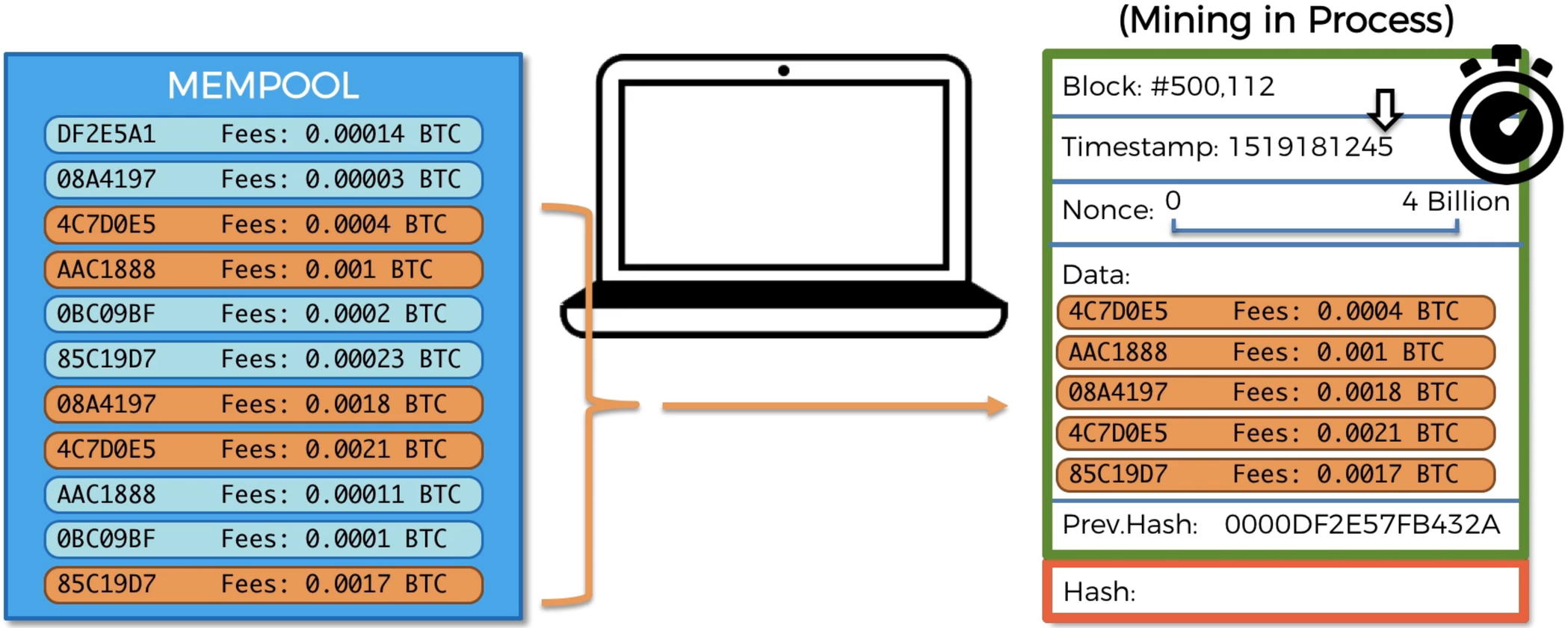
←유닉스 타임
-1초마다 갱신!

타임이 바뀌기 때문에 찾아야 하는 nonce값이 다시 갱신됨@@!

논스 범위인 40억의 경우의 수를 1초도 안걸려서 다 해볼수 있는 채굴자가 있다면..?

네트워크의 전체 해시율은 초당 2200만조....

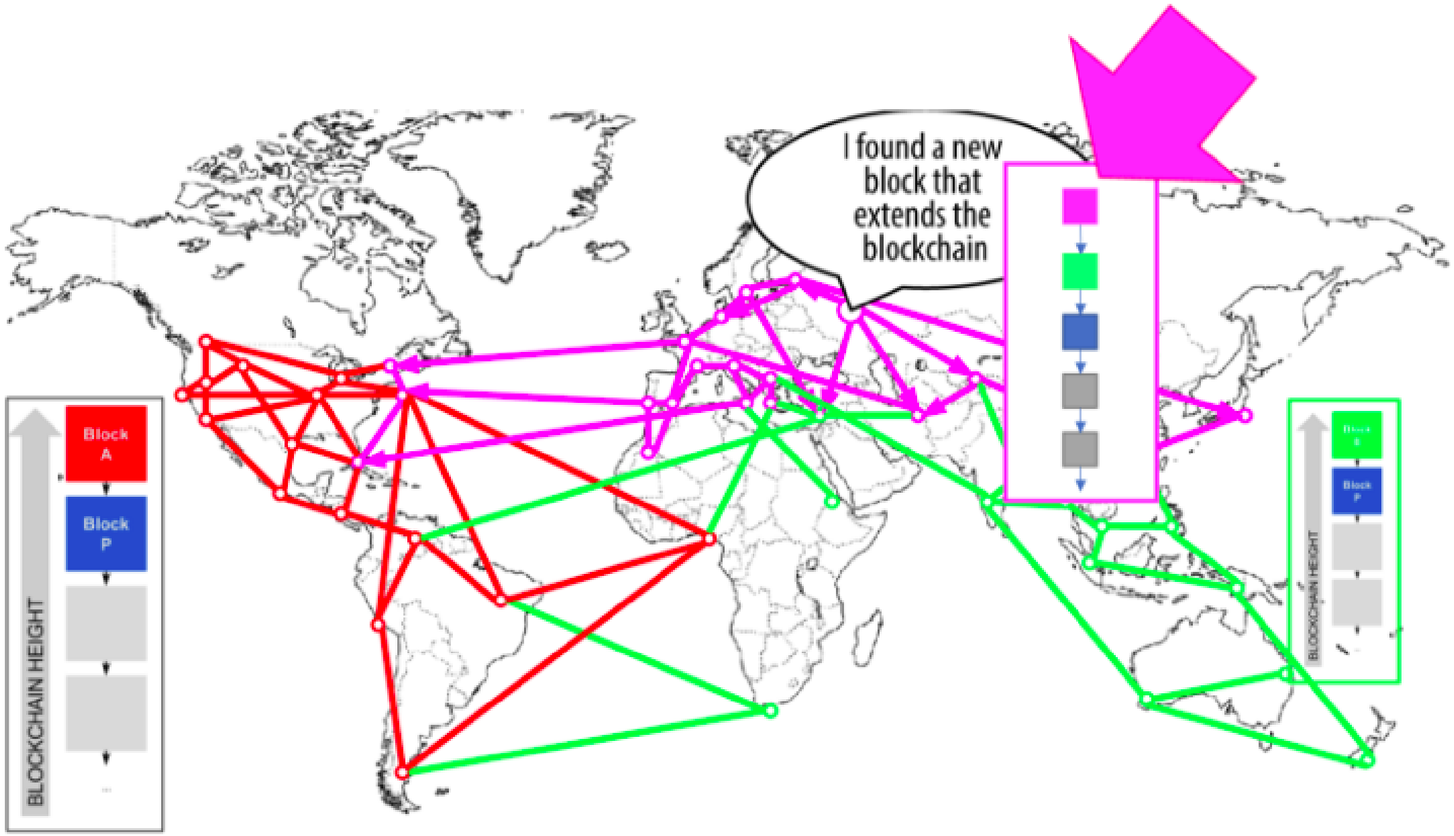
채굴



채굴자는 대기중인 트랜잭션중에 노드에 포함할 것을 고름. 당연히 수수료 높은 순으로 고를거임

머클루트가 달라지기에 다시 노가다!

블록당 약 2000개의 트랜잭션(거래) 가짐-1MB



빨간색 채굴자 우야누??

위와 같이 파란색 블록을 마지막으로 비슷한 시기에 한쪽은 빨간색, 한쪽은 초록색 블록을 채굴하여 체인이 2개로 분기가 됐다고 가정해보자.
이 상태에서 각각의 노드는 peer network로 블록을 전파할 것이고
(그림에선 지리학적으로 가까운 곳부터 전파되는 것처럼 보이지만, 실제로는 토폴리지 구성상 가까운 곳부터 이다.)
주변의 노드들은 먼저 전파 받은 체인을 각각 유지하는 형태가 될 것이다.
이 상태에서 초록색 블록까지 동기화한 곳에서 새로 분홍색 블록이 채굴됐다면,
전파 받는 곳에선 빨간색 블록을 받아도 이는 무시되고, 분홍색 블록이 담긴 체인을 메인체인으로 유지할 것이다.
그렇다면 기존에 빨간색 블록을 메인체인으로 유지하고 있던 노드는 어떻게 될 것인가?
분홍색 체인을 받는 순간 누적 난이도가 더 높은 분홍색 체인을 메인체인으로 채택하고, 기존 빨간 블록체인은 2차체인으로 변경할 것이다(고급용어로 포크).
이렇게 더 이상 이후로 쌓이지 않는 이러한 빨간색 블록을 고아블록(나가 떨어지는 블록)이라고 부른다.

보상을 그래서 바로 안줌!!

보상은 100블록이 쌓일 때까지 잠금 상태
100블록이면 약 16~17시간 정도(10분 × 100)
이 기간이 지나면 해당 블록이 거의 확정되었다고 봐도 안전
이렇게 하면 포크가 일어나도, 이미 쓴 보상이 무효가 되는 문제를 예방 가능

그럼 고아 블록에 있는 거래 기록은 없어짐??

MEMPOOL 또한 동기화가 되기 때문에, 해당 트랜잭션이 유실되는 일은 발생X
누적 난이도가 더 높은 분홍체인(더 길에 유지되고 있는 체인)에
빨간 블록의 트랜잭션이 이미 포함되어 있을 가능성이 매우 높고,
그렇지 않다고 하더라도 MEMPOOL 에 들어있기 때문에
블록에 기록되는 우선순위가 늦어지는 것일 뿐 언젠가는 블록에 포함됨.
유효한 트랜잭션이 맞다면, 유실될 걱정은 X

Bitcoin Block 909,524

Mined on August 11, 2025 03:47:45 • All Blocks

Unknown

Coinbase Message • ,z>mm+ G}o"ᒧ ‼$6X_,Ab┤┴┬2jD8gD–wKYLVN•┼ p₹╪₹ /F2Pool/d | ♀\ s

A total of 9,252.34 BTC ($1,130,379,437) were sent in the block with the average transaction being 3.1396 BTC ($383,572). Unknown earned a total reward of 3.13 BTC $382,399. The reward consisted of a base reward of 3.13 BTC $382,399 with an additional 0.0310 BTC ($3,787.34) reward paid as fees of the 2,947 transactions which were included in the block.

Details

Hash	00000-2dca4	Depth	1
Capacity	159.31%	Size	1,670,482
Distance	5m 12s	Version	0×20150000
BTC	9,252.3352	Merkle Root	85-5a
Value	$1,130,379,437	Difficulty	129,435,235,580,344.81
Value Today	$1,130,654,787	Nonce	2,603,383,110
Average Value	3.1395775927 BTC	Bits	386,018,483
Median Value	0.00222729 BTC	Weight	3,960,352 WU
Input Value	9,252.37 BTC	Minted	3.13 BTC
Output Value	9,255.49 BTC	Reward	3.15596804 BTC
Transactions	2,947	Mined on	2025년 8월 11일 오후 3:47:45
Witness Tx's	2,742	Height	909,524
Inputs	9,087	Confirmations	1
Outputs	7,268	Fee Range	0-252 sat/vByte
Fees	0.03096804 BTC	Average Fee	0.00001051
Fees Kb	0.0000185 BTC	Median Fee	0.00000366
Fees kWU	0.0000078 BTC	Miner	Unknown

Blockchain

#909524 #909523 #909522 #909521 #909520 #909519 #909518 #909517 #909516 #909515 #909514 #909513

Transactions

Last | First | ↗ Value | ↘ Value | ↗ Fee | ↘ Fee

0	ID: 3718-1aba 8/11/2025, 15:47:45	From Block Reward To 8 Outputs	3.15596804 BTC • $385,572 Fee 0 Sats • $0.00
TX	1 ID: fb99-6de3 8/11/2025, 15:34:58	From 3 Inputs To 36vY-DbmD	0.33418780 BTC • $40,828.51 Fee 123.5K Sats • $150.88
TX	2 ID: 1093-8150 8/11/2025, 15:37:24	From bc1q-vzej To 2 Outputs	0.99940000 BTC • $122,099 Fee 60.0K Sats • $73.30
TX	3 ID: ced0-3d82 8/11/2025, 15:41:31	From bc1q-xw2k To 2 Outputs	0.12628922 BTC • $15,429.05 Fee 28.2K Sats • $34.45
TX	4 ID: ed60-ed7f 8/11/2025, 15:45:03	From 3DGx-wTJF To 2 Outputs	0.01977285 BTC • $2,415.70 Fee 22.2K Sats • $27.18
TX	5 ID: 35d5-b8b7 8/11/2025, 15:47:45	From bc1q-cvrs To bc1q-hfje	0.99979000 BTC • $122,146 Fee 11.0K Sats • $13.44
TX	6 ID: 2c62-03fe 8/11/2025, 15:45:54	From bc1p-l8tt To bc1p-xgwt	0.00468000 BTC • $571.77 Fee 32.0K Sats • $39.10
TX	7 ID: e52d-f11a 8/11/2025, 15:43:47	From bc1q-tf4s To 2 Outputs	0.01226156 BTC • $1,498.02 Fee 12.0K Sats • $14.66
TX	8 ID: 3204-b82f 8/11/2025, 15:35:06	From bc1q-gqsj To 2 Outputs	0.86482000 BTC • $105,657 Fee 9.9K Sats • $12.10
TX	9 ID: b9d5-b991 8/11/2025, 15:35:13	From 7 Inputs To 2 Outputs	30.35675880 BTC • $3,708,756 Fee 48.8K Sats • $59.60
TX	10 ID: 1e6c-6dc2 8/11/2025, 15:46:53	From bc1q-vzej To 6 Outputs	0.29020860 BTC • $35,455.46 Fee 18.9K Sats • $23.09

https://www.blockchain.com/explorer/blocks/btc?page=1

https://www.ledger.com/ko/academy/%EC%A7%80%EB%B6%84-%EC%A6%9D%EB%AA%85%EC%9D%B4%EB%9E%80

PoW vs PoS

작업증명 지분증명

ethereum

지분 증명

새 블록을 검증할 확률은 사람이 보유한 지분의 크기에 따라 결정됩니다.

검증인은 블록 보상을 받지 않고 대신 네트워크 수수료를 보상으로 연결합니다.

지분 증명 시스템은 작업 증명보다 훨씬 더 비용과 에너지 효율이 높을 수 있지만 덜 입증되었습니다.

최소 32개의 이더리움을 스테이킹(예치)하면 밸리데이터가 되서 노드를 운영할 수 있음.
이더리움 네트워크는 트랜잭션 검증을 밸리데이터에게 맡기는데, 무작위로 밸리데이터를 선정.
그런데 더 많은 이더를 보유한 사람이 검증인으로 선택될 확률이 더 높음.
쉽게 말해 더 많은 이더 지분을 보유할수록 더 많은 보상을 받는 것이 지분증명.

Thank you