Blockchain and Digital Currencies

Lecture 10

PHBS 2024 M3

Agenda

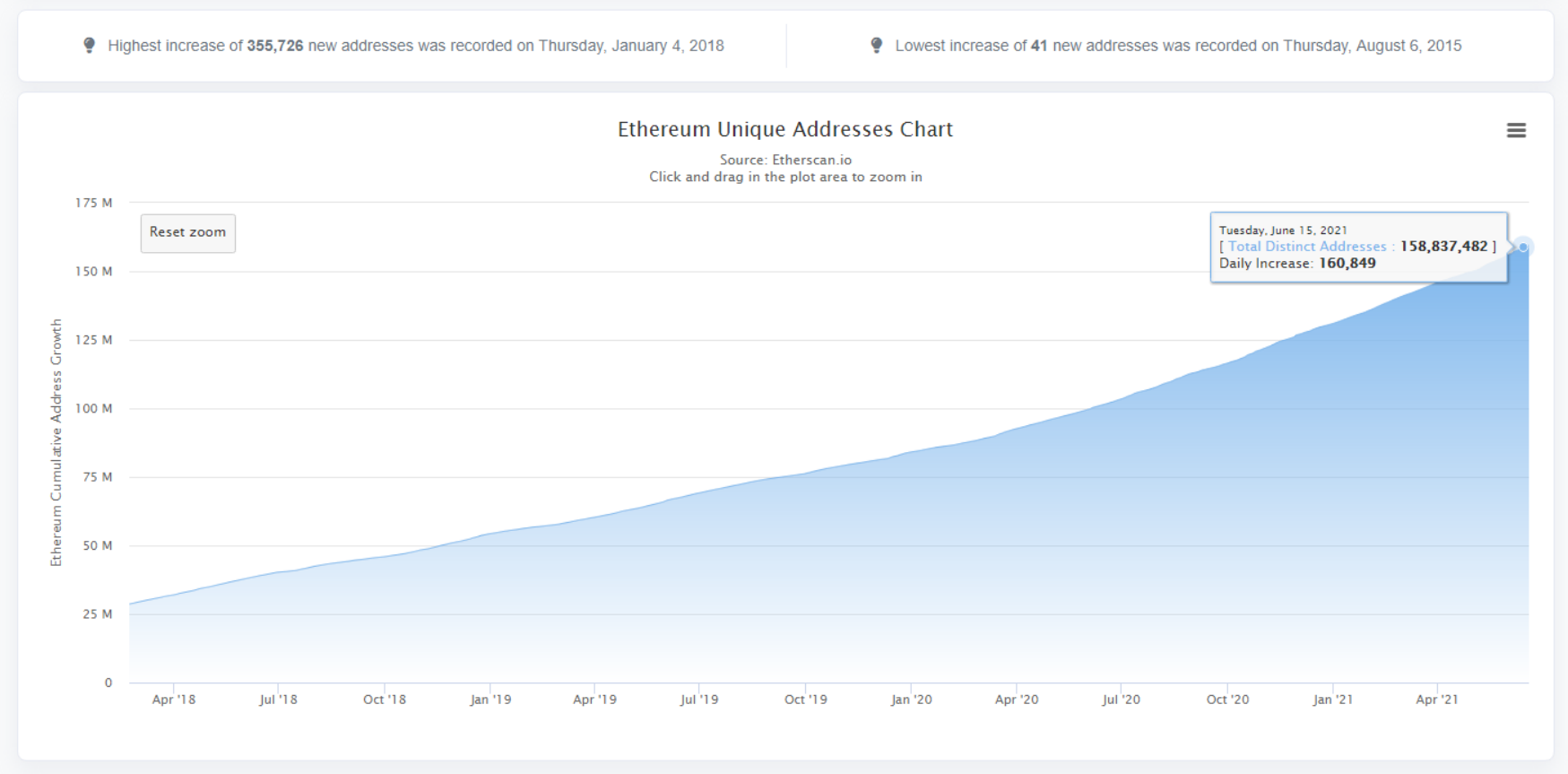
- Ethereum Mining
- Uncle Blocks

Review Questions

- Suppose you are an ETH miner, is it possible for you to see a new account that you have never seen before?
  - Yes. An EOA or contract account?
  - What to do if a new account is identified?
- The size difference between state trie, transaction trie, and receipt trie?
  - A state trie contains the states of all accounts, while a transaction trie and a receipt trie only refer to the transactions included in the same block.

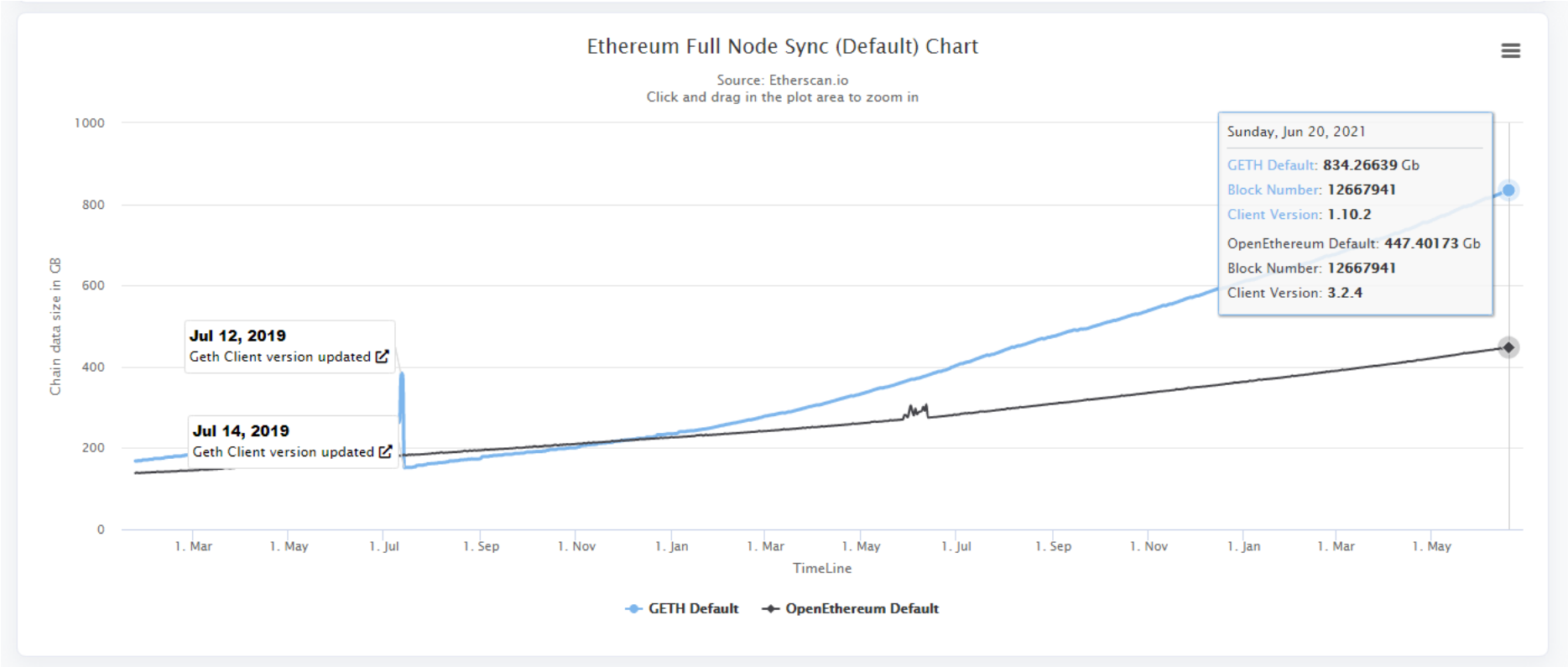
Address Growth of Ethereum

- The number of Ethereum addresses keeps growing https://etherscan.io/chart/address



Storage Size Growth of Full Node

- The storage size of Ethereum full node keeps growing https://etherscan.io/chartsync/chaindefault



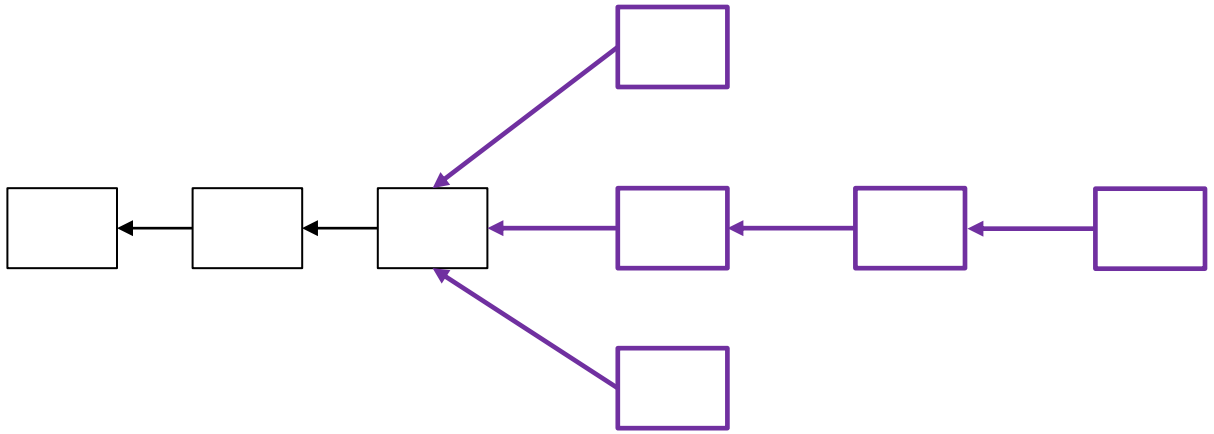
Design of State Trie Revisited

- Given a block, let the state trie only store the accounts affected by the transactions included in the block
  - This design is simpler but causes problems
  - Need to verify that the sender account has enough money
  - Need to add the transfer money to the receipt account
  - The problem is that it takes time to locate which blocks contain the sender account and receipt account
  - What if the receipt account is a new one?
  - Comparing to Bitcoin, only input coins need to be verified, and only when input coins are used.

Mining Revisited

- Bitcoin blockchain: one block every 10 minutes on average
  - Multiple valid blocks may be generated around the same time, and the network delay causes race conditions
  - Which block to choose is up to miners (individual vs. mining pools)
  - The discarded blocks indicate waste of energy and money
- Ethereum blockchain: one block every 15 seconds on average
  - An obvious advantage is much higher throughput (flow rate)
  - However more chances to create conflicts
  - Can we take more blocks into the main blockchain?

Mining Centralization Bias



The chance of a miner to get a valid block is proportional to his/her mining power; however, the chance of the miner to get reward is much higher if he/her has much more mining power than others.

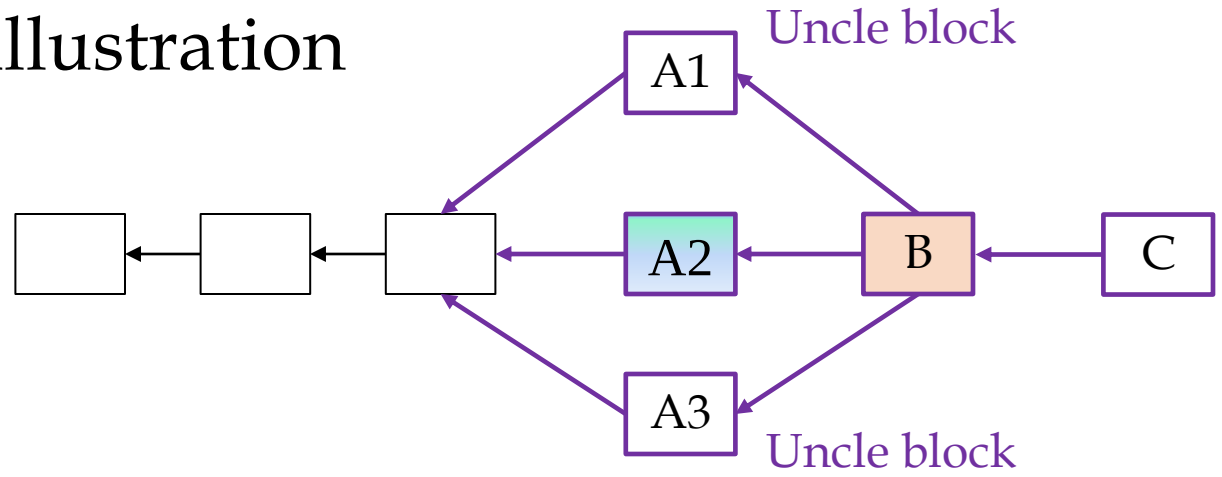
The consensus here has to take perception into consideration.

GHOST Protocol

- GHOST: Greedy Heaviest Object Sub Tree
  - Yonatan Sompolinsky and Aviv Zohar December, 2013
  - Does not choose necessarily the longest branch
  - Evaluates if the root of the subtrees should be part of the branch that is decided
  - Also award blocks not taken into the longest branch
- To absorb forks as much as possible, as quickly as possible
- To encourage all miners to work together on the same blockchain

GHOST Protocol

- Graphic illustration



A1 and A3 are Uncle blocks for B, while A2 is the parent block for B

When B block is mined, A1 and A3 can be included as uncles, so that both miners of A1 and A3 will be rewarded together with B's miner.

Miners of A1 and A3 get 7/8 * static block reward (2 as of 2021/06)
Miner of B get 1/32 * static block reward for each uncle block

One Example (From https://etherscan.io/blocks)

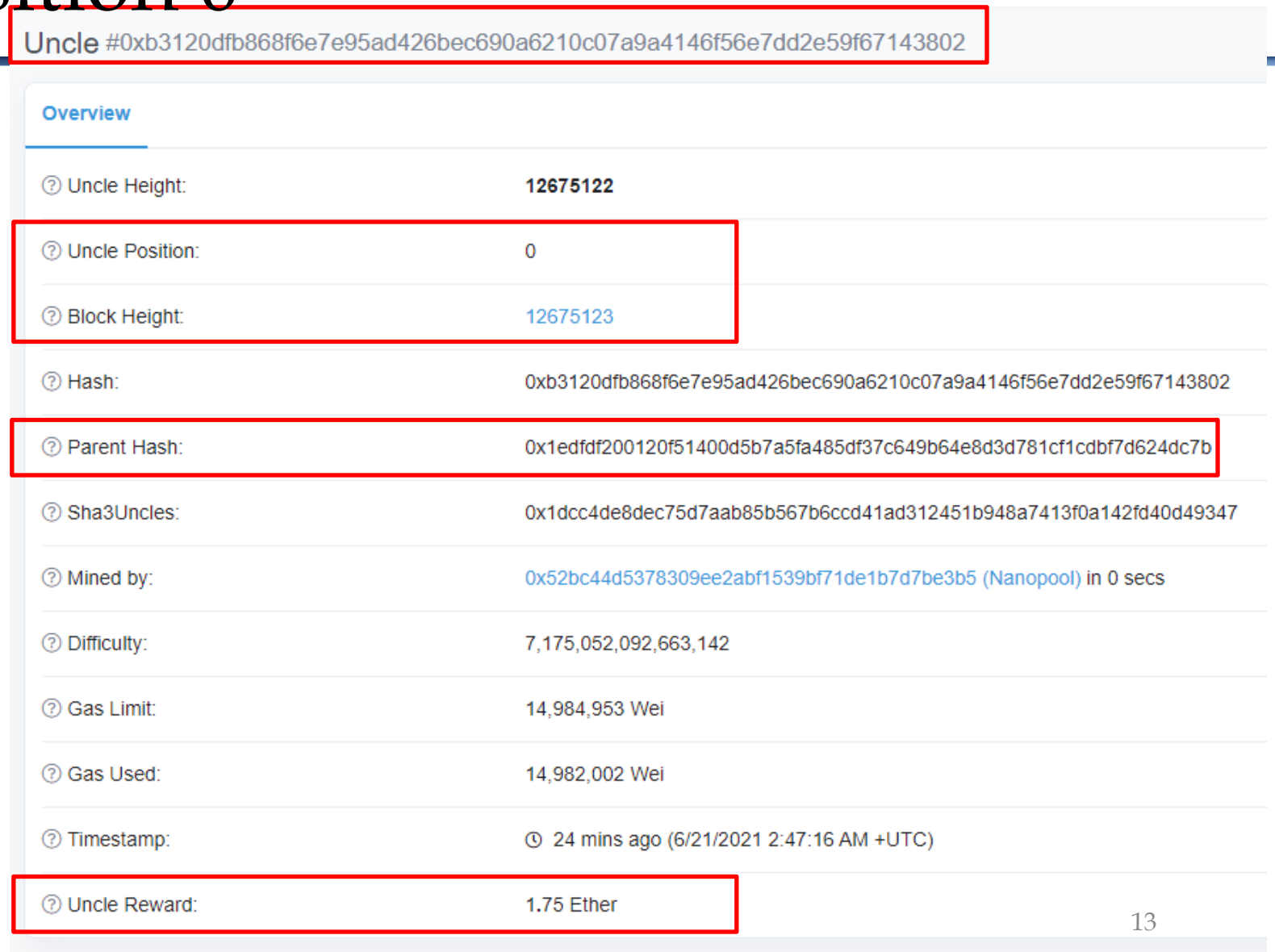
Block #12675029 to #12675128 (Total of 12,675,129 blocks)

First | < | Page 1 of 126752 | > | Last

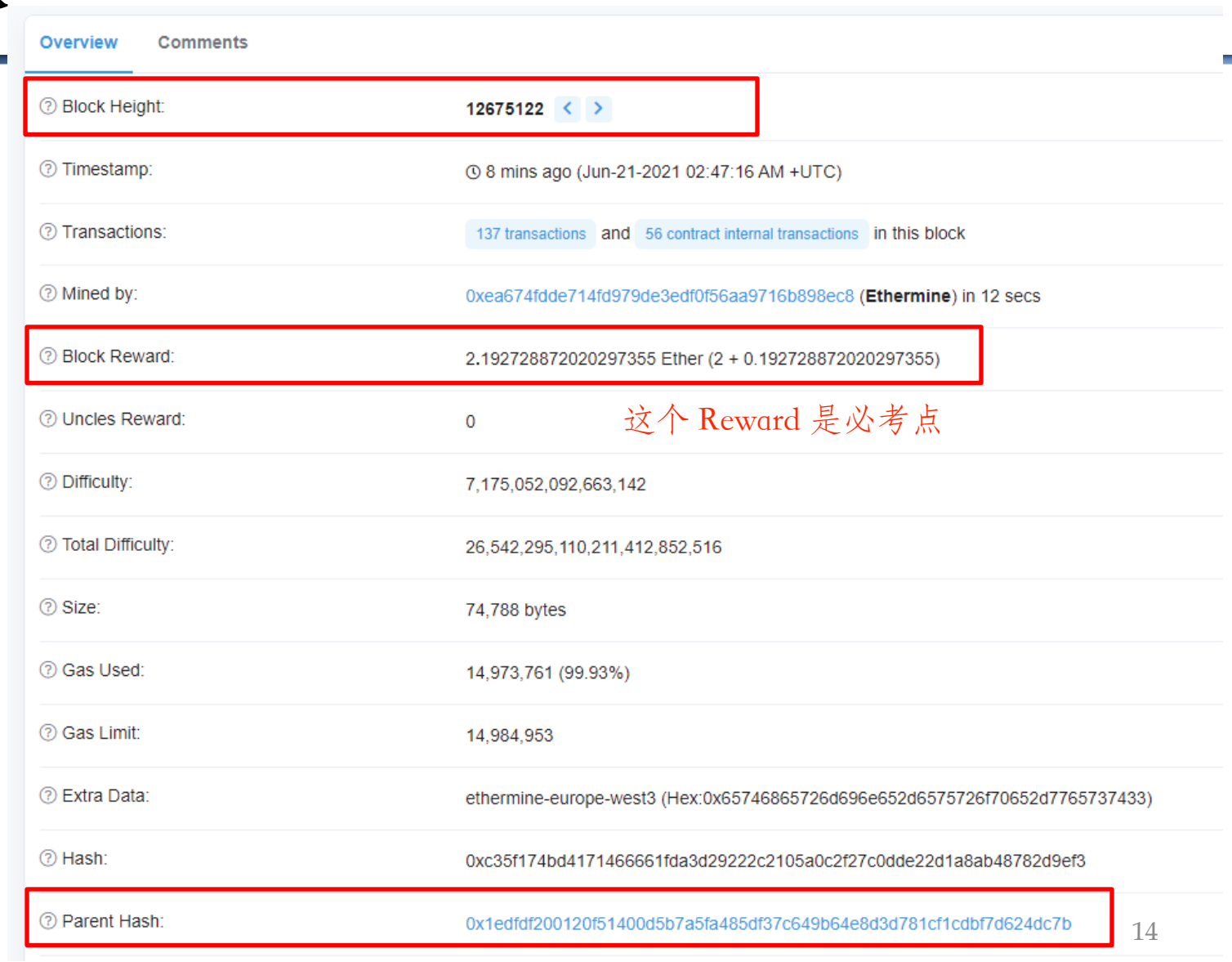
Block	Age	Txn	Uncles	Miner	Gas Used	Gas Limit	Avg.Gas Price	Reward
12675128	25 secs ago	170	0	Spark Pool	14,964,089 (99.91%)	14,977,601	16.14 Gwei	2.2415 Ether
12675127	50 secs ago	171	0	0x21479eb8cb1a27861c...	14,969,375 (99.99%)	14,970,292	17.85 Gwei	2.26724 Ether
12675126	1 min ago	430	0	BeePool	14,969,803 (99.90%)	14,984,924	11.73 Gwei	2.17555 Ether
12675125	1 min ago	144	0	0x21479eb8cb1a27861c...	14,963,466 (99.95%)	14,970,306	21.11 Gwei	2.31581 Ether
12675124	1 min ago	155	0	Hiveon Pool	14,979,245 (99.96%)	14,984,938	15.00 Gwei	2.22465 Ether
12675123	2 mins ago	180	1	Ethermine	14,978,992 (99.86%)	14,999,585	18.43 Gwei	2.33862 Ether
12675122	2 mins ago	137	0	Ethermine	14,973,761 (99.93%)	14,984,953	12.87 Gwei	2.19272 Ether
12675121	2 mins ago	131	0	Ethermine	14,954,493 (99.89%)	14,970,335	16.67 Gwei	2.24929 Ether
12675120	3 mins ago	206	0	EzilPool 2	14,952,040 (99.98%)	14,955,731	17.24 Gwei	2.25773 Ether
12675119	3 mins ago	133	0	MiningPoolHub	14,957,822 (99.92%)	14,970,349	12.72 Gwei	2.19023 Ether
12675118	3 mins ago	153	0	Ethermine	14,979,064 (99.96%)	14,984,981	15.39 Gwei	2.23046 Ether
12675117	3 mins ago	178	0	Ethermine	14,980,160 (99.87%)	14,999,628	14.15 Gwei	2.21201 Ether

One Example Continued (https://etherscan.io/block/12675123)

The Uncle at Position 0



The Parent Block



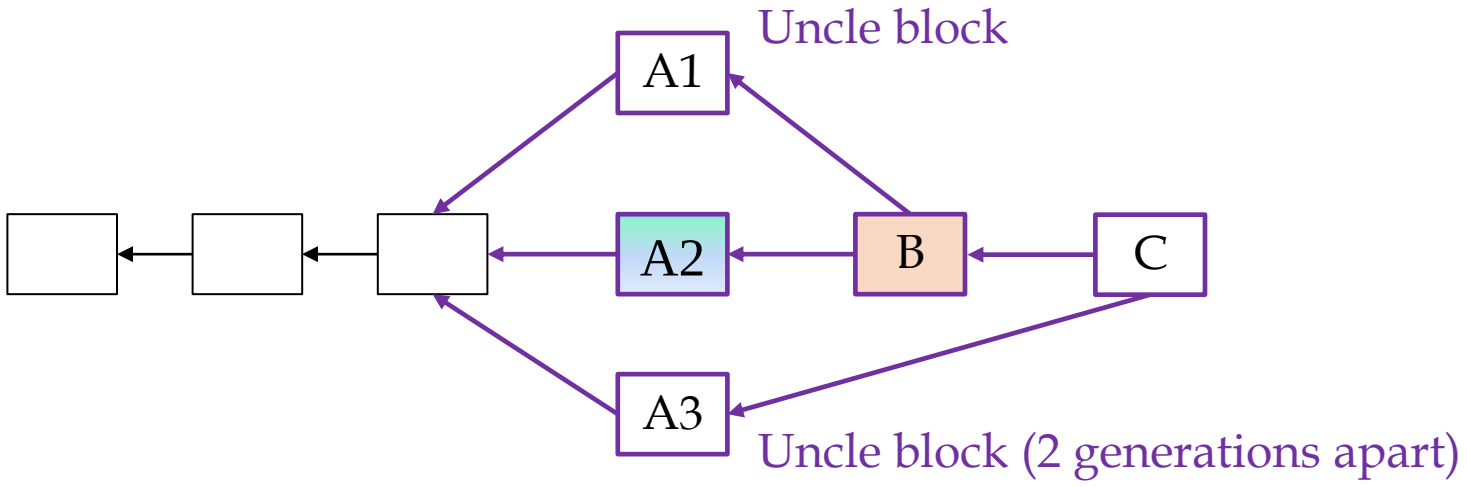
Overview | Comments

Block Height:	12675122
Timestamp:	8 mins ago (Jun-21-2021 02:47:16 AM +UTC)
Transactions:	137 transactions and 56 contract internal transactions in this block
Mined by:	0xea674fdde714fd979de3edf0f56aa9716b898ec8 (**Ethermine**) in 12 secs
Block Reward:	2.192728872020297355 Ether (2 + 0.192728872020297355)
Uncles Reward:	0
Difficulty:	7,175,052,092,663,142
Total Difficulty:	26,542,295,110,211,412,852,516
Size:	74,788 bytes
Gas Used:	14,973,761 (99.93%)
Gas Limit:	14,984,953
Extra Data:	ethermine-europe-west3 (Hex:0x65746865726d696e652d6575726f70652d7765737433)
Hash:	0xc35f174bd4171466661fda3d29222c2105a0c2f27c0dde22d1a8ab48782d9ef3
Parent Hash:	0x1edfdf200120f51400d5b7a5fa485df37c649b64e8d3d781cf1cdbf7d624dc7b

这个 Reward 是必考点

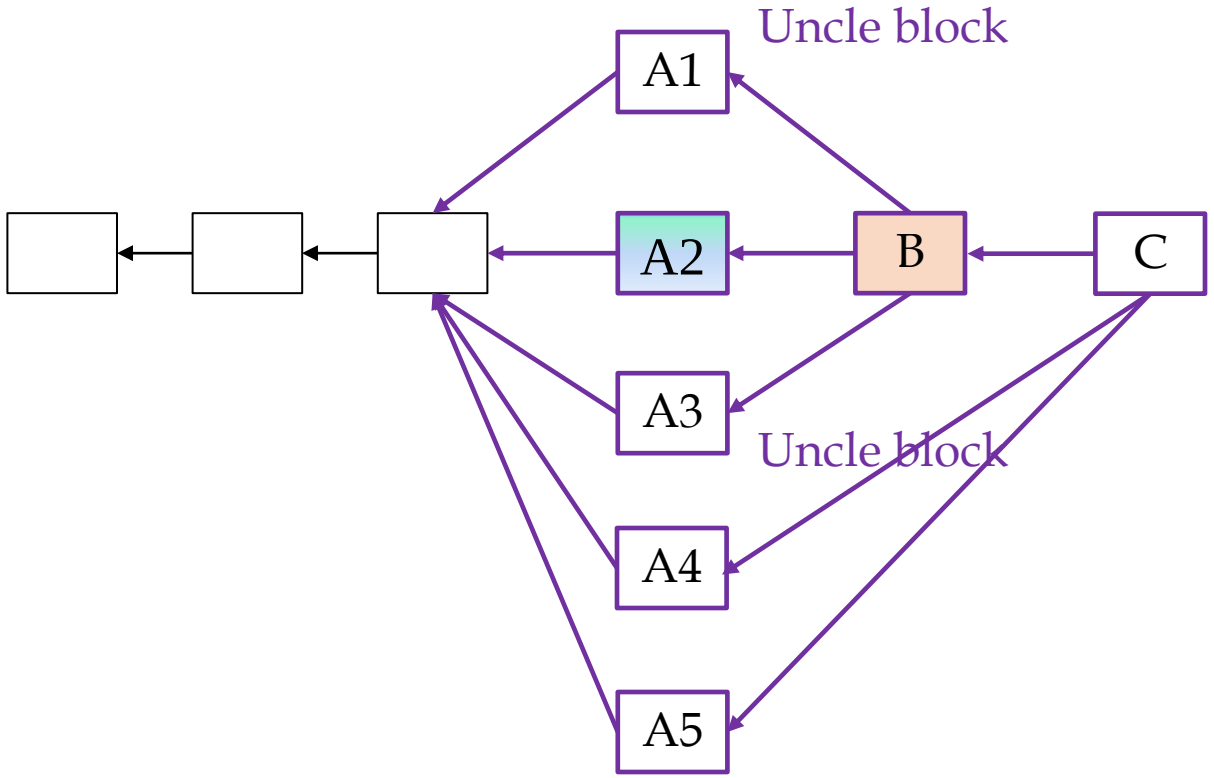
Any Exploits?

- Which uncle block to be included?
  - The competition among miners may still encourage miners to discard uncle blocks intentionally (7/8 loss vs 1/32 loss)
  - Solution: A miner can harvest its own uncle block if needed (for example, the miner of A3 will include A3 when mining C)



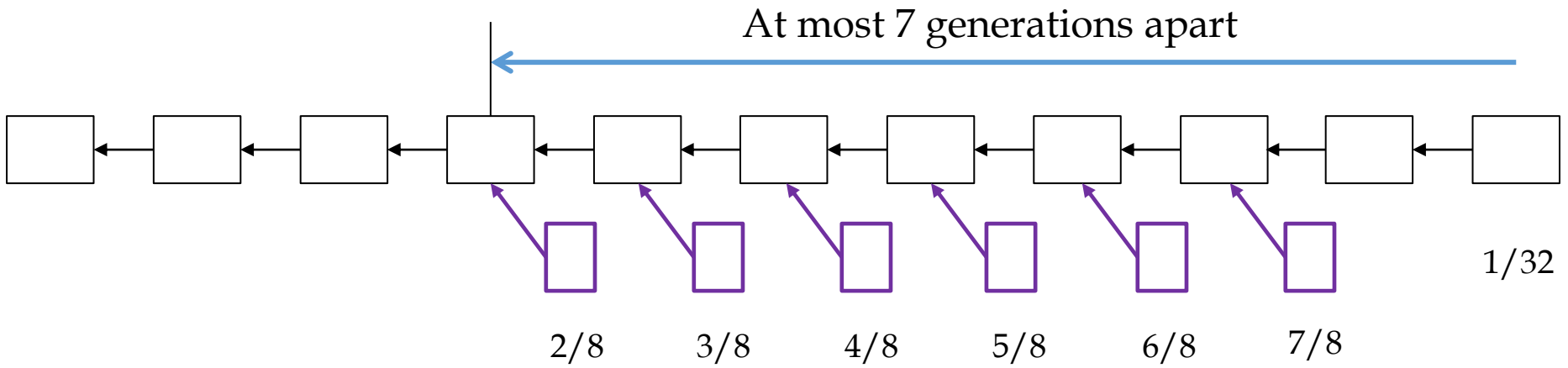
Uncle Blocks With Several Generations Apart

- At most two uncle blocks can be included, what if multiple uncle blocks exist?
  - Any main chain block can take up to 2 uncle blocks



Any More Exploits?

- Is there anyway to create many uncle blocks with little efforts?
  - Go upstream and create uncle blocks at the very beginning of the main blockchain when difficulty level is low
  - Solution: the reward of uncle blocks diminish to 0 over the last 7 generations
    - To reduce storage cost and encourage uncle block inclusion



Uncle Block Treatment

- A block still has to be validated to be qualified as an uncle block
- All transaction in an uncle block will be discarded (why?)
  - As can be seen from slide page 12
  - The transactions not included in the main blockchain will have to be mined by other miners
  - Therefore no transaction fee reward for uncle blocks
- What about the blocks after the uncle block?
  - Discarded with no reward at all
  - Discourage forking and attack (draw an graph)
- To keep the Ethereum system simple and robust!

Block Height	UncleNumber	Age	Miner	Reward	
5695161	5695159	4 mins ago	f2pool_2	2.25 Ether	#1
5695159	5695157	5 mins ago	miningpoolhub_1	2.25 Ether	
5695157	5695155	6 mins ago	0xb6b12f9f4ed7c57...	2.25 Ether	
5695154	5695153	7 mins ago	Ethermine	2.625 Ether	#2
5695150	5695148	8 mins ago	bitclubpool	2.25 Ether	
5695150	5695149	8 mins ago	f2pool_2	2.625 Ether	
5695142	5695141	9 mins ago	Nanopool	2.625 Ether	
5695133	5695131	11 mins ago	f2pool_2	2.25 Ether	
5695129	5695128	12 mins ago	Nanopool	2.625 Ether	
5695119	5695118	15 mins ago	0x92e3f585ab69944...	2.625 Ether	
5695113	5695111	16 mins ago	Nanopool	2.25 Ether	
5695109	5695106	17 mins ago	DwarfPool1	1.875 Ether	#3

Source:Etherscan.io

距离	比例	实际奖励	示例
1	7/8	2.625	#2
2	6/8	2.25	#1
3	5/8	1.875	#3
4	4/8	1.5	
5	3/8	1.125	
6	2/8	0.75	

Example from Professor Xiao
Note: the block reward is 3 Eths

Uncle Blocks in https://etherscan.io/uncles

Most blocks are mined following the main blockchain.

Most uncle blocks are mined within one generation.

Very few blocks are mined with 2 or more generations. Note block reward = 2 Ethers

12675025	12675024	54 mins ago	2Miners: PPLNS	1.75 Ether
12675017	12675016	55 mins ago	zhizhu.top	1.75 Ether
12674997	12674996	1 hr ago	Nanopool	1.75 Ether
12674982	12674980	1 hr 4 mins ago	Spark Pool	1.5 Ether
12674919	12674918	1 hr 17 mins ago	Hiveon Pool	1.75 Ether
12674871	12674870	1 hr 30 mins ago	Hiveon Pool	1.75 Ether
12674855	12674854	1 hr 34 mins ago	Nanopool	1.75 Ether
12674837	12674836	1 hr 38 mins ago	Ethermine	1.75 Ether
12674836	12674835	1 hr 38 mins ago	F2Pool Old	1.75 Ether
12674824	12674823	1 hr 41 mins ago	Spark Pool	1.75 Ether
12674813	12674811	1 hr 43 mins ago	F2Pool Old	1.5 Ether
12674793	12674792	1 hr 46 mins ago	BeePool	1.75 Ether
12674718	12674716	2 hrs 2 mins ago	Babel Pool	1.5 Ether

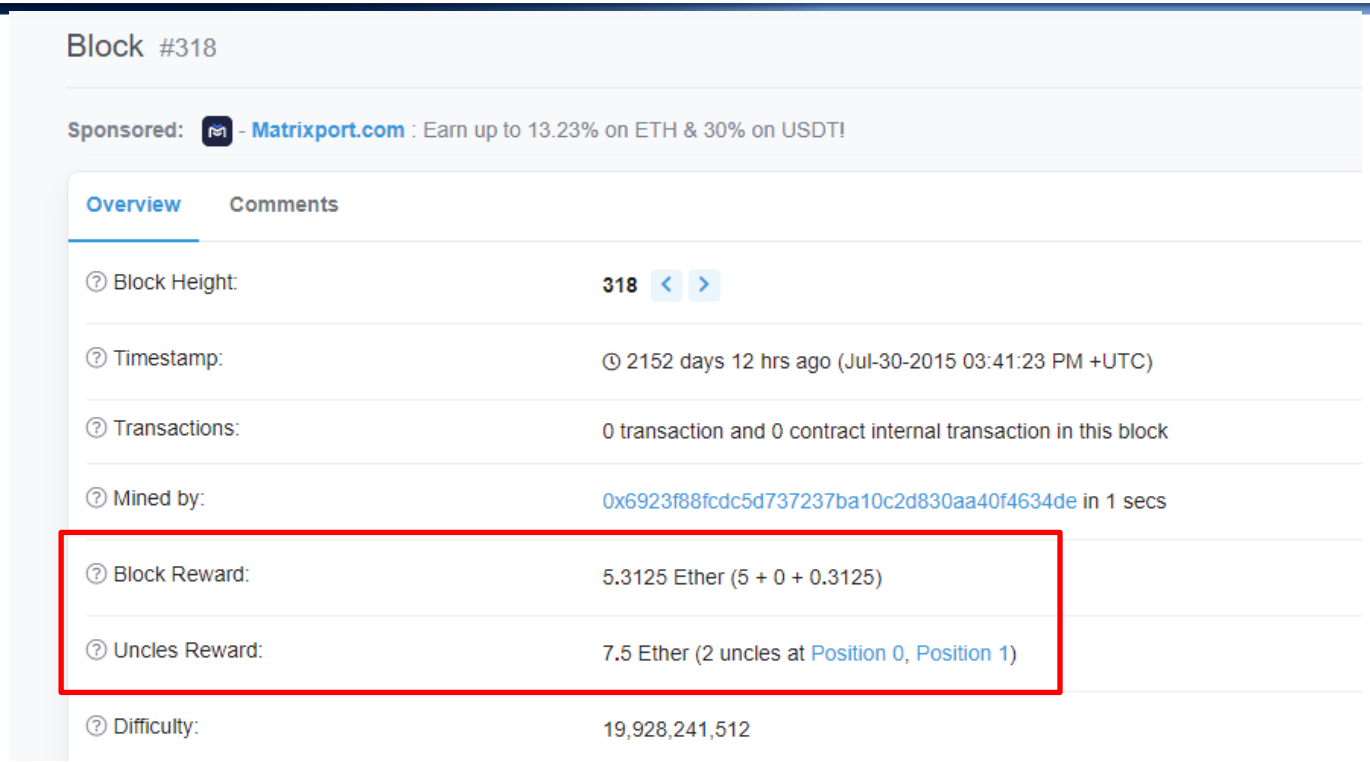
Uncle Blocks in https://etherscan.io/uncles

In the early days, it is easy to see uncle blocks with more than 2 generations apart.

For example: block 231 takes block 225 as the uncle block and get reward as 2/8*5 = 1.25, where 2/8 comes from 6 generations apart. Note block reward = 5 Ethers

268	264	2152 days 12 hrs ago	0xfb7bc66a002762e28545ea0a7fc970d381863c42	2.5 Ether
264	262	2152 days 12 hrs ago	0x6923f88fcdc5d737237ba10c2d830aa40f4634de	3.75 Ether
259	257	2152 days 12 hrs ago	0x1b7047b4338acf65be94c1a3e8c5c9338ad7d67c	3.75 Ether
256	253	2152 days 12 hrs ago	0xbb7b8287f3f0a933474a79eae42cbca977791171	3.125 Ether
254	250	2152 days 12 hrs ago	0x28921e4e2c9d84f4c0f0c0ceb991f45751a0fe93	2.5 Ether
251	249	2152 days 12 hrs ago	0xbb7b8287f3f0a933474a79eae42cbca977791171	3.75 Ether
247	244	2152 days 12 hrs ago	0x05a56e2d52c817161883f50c441c3228cfe54d9f	3.125 Ether
243	238	2152 days 12 hrs ago	0xefcd857c9235bdd977b33b263dbb0255f055aad5	1.875 Ether
241	239	2152 days 12 hrs ago	0x28921e4e2c9d84f4c0f0c0ceb991f45751a0fe93	3.75 Ether
238	233	2152 days 12 hrs ago	0x28921e4e2c9d84f4c0f0c0ceb991f45751a0fe93	1.875 Ether
231	225	2152 days 12 hrs ago	0x5088d623ba0fcf0131e0897a91734a4d83596aa0	1.25 Ether
229	227	2152 days 12 hrs ago	0x1b7047b4338acf65be94c1a3e8c5c9338ad7d67c	3.75 Ether

Two Uncle Blocks



2*1/32*5 = 0.3125

326	324	2152 days 12 hrs ago	0x48cd680bb700f6b7de89dd9ff4932ccc158c3e05	3.75 Ether
324	321	2152 days 12 hrs ago	0x28921e4e2c9d84f4c0f0c0ceb991f45751a0fe93	3.125 Ether
318	316	2152 days 12 hrs ago	0xd7e30ae310c1d1800f5b641baa7af95b2e1fd98c	3.75 Ether
318	316	2152 days 12 hrs ago	0x0193d941b50d91be6567c7ee1c0fe7af498b4137	3.75 Ether
313	311	2152 days 12 hrs ago	0xbb7b8287f3f0a933474a79eae42cbca977791171	3.75 Ether

Disclaimer

- The purpose of this lecture is only for us to understand the underlying mechanism of mining
- We DO NOT encourage you to mine any cryptocurrencies
- As matter of fact, we should always obey the laws and policies

History Event in 2021

时代落幕：四川比特币矿场今晨集体断电，世界最大的矿工聚集地或将走向终结

21财闻汇 昨天

继内蒙古、青海等地之后，水电资源丰富、聚集了众多虚拟货币矿场的四川省也开启清退虚拟货币挖矿项目。多名加密货币从业者前几日表示，中国比特币矿业很快将迎来历史性时刻。

据电商报，6月20日零点，四川所有比特币等虚拟货币矿机将被集体断电，来不及转移的比特币矿工因此遭受巨大损失。

据南财快讯此前消息，6月18日，一份《四川省发展和改革委员会、四川省能源局关于清理关停虚拟货币"挖矿"项目的通知》文件在网上流出，通知要求各市（州）于6月20日前完成省内26个疑似虚拟货币挖矿重点项目的甄别、清理和关停工作，同时要求发电企业立即停止向虚拟货币挖矿项目供电，并于6月25日前上报自查、整改情况。此外，各市（州）政府也被要求开展拉网式排查，对发现的挖矿项目立即关停。

Alternative Puzzle Choice

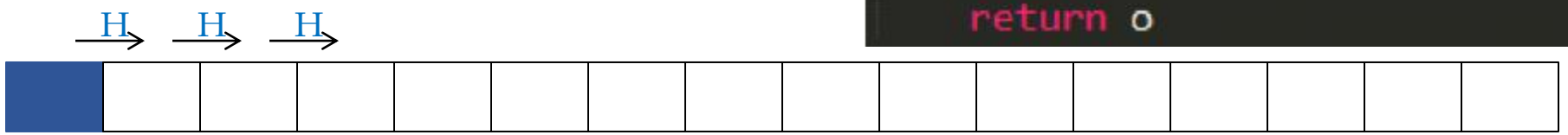
PM

- ASIC (Application-Specific Integrated Circuit) mining machines
- ASIC resistance – memory hard mining puzzle
- Possible solutions: E.G. Scrypt
  - Force hash functions to read memory instead of registers only
  - Require a large set of memory to save path dependent information (recursive algorithm), time memory tradeoff
- Issues: also very difficult to verify ☹

Ethereum Mining Algorithm

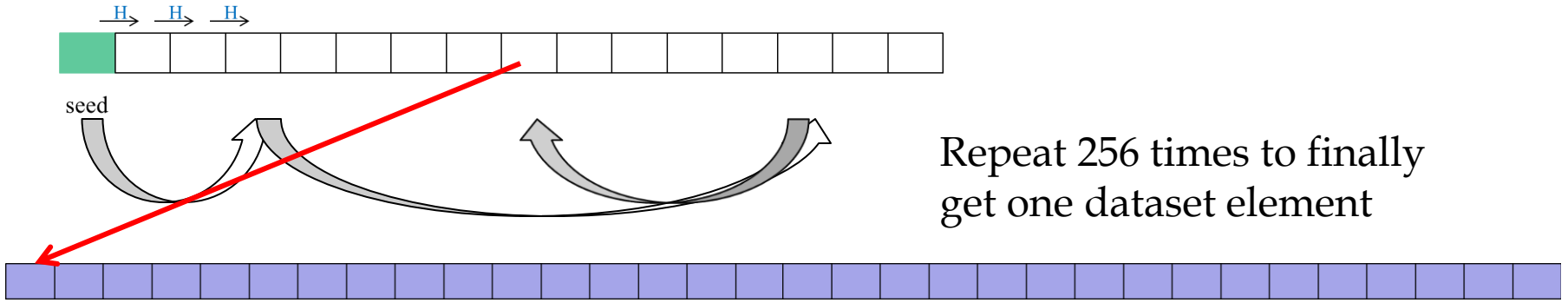
- Two data sets:
  - Cache 16M: easy for light nodes to verify blocks
  - Dataset 1G: generated from Cache, used by full nodes
- Three steps:
  - Step I:
  - Generate 16M cache, starting with a random seed and generate values in sequence using hash functions

```
def mkcache(cache_size, seed):
    o = [hash(seed)]
    for i in range(1, cache_size):
        o.append(hash(o[-1]))
    return o
```



Ethereum Mining Algorithm II

- Step II: generate dataset
  - Utilizing the elements in the Cache and hash values of these elements to calculate element in dataset



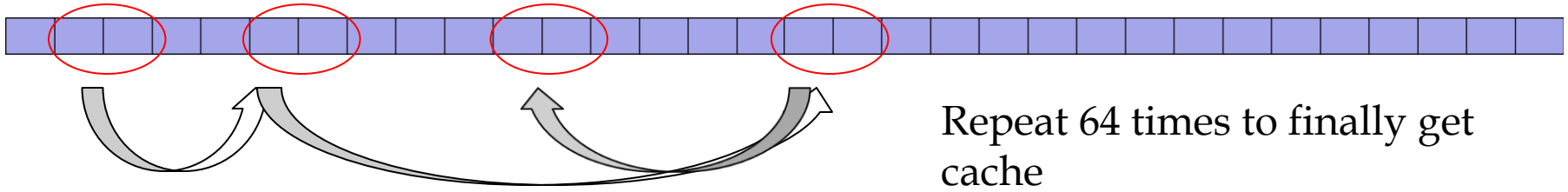
Repeat 256 times to finally get one dataset element

```
def calc_dataset_item(cache, i):
    cache_size = cache.size
    mix = hash(cache[i % cache_size] ^ i)
    for j in range(256):
        cache_index = get_int_from_item(mix)
        mix = make_item(mix, cache[cache_index % cache_size])
    return hash(mix)
```

Ethereum Mining Algorithm III

AM

- Step III: finding nonce meeting difficulty
  - Use the given nonce to find 128 elements in the dataset and calculate their hash to see it meets difficulty level

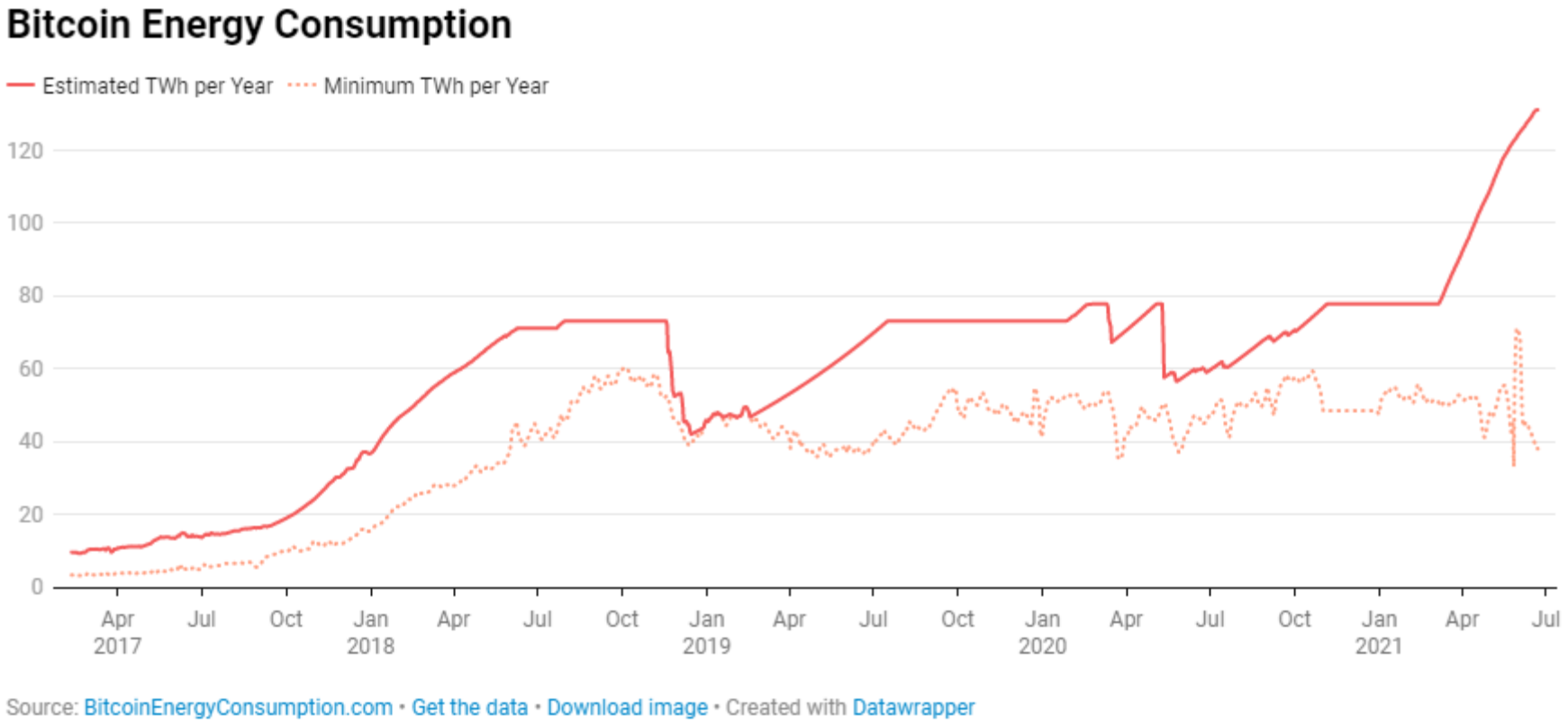


Repeat 64 times to finally get cache
Each time 2 elements are selected.

```
def hashimoto_full(header, nonce, full_size, dataset):
    mix = hash(header, nonce)
    for i in range(64):
        dataset_index = get_int_from_item(mix) % full_size
        mix = make_item(mix, dataset[dataset_index])
        mix = make_item(mix, dataset[dataset_index + 1])
    return hash(mix)
```

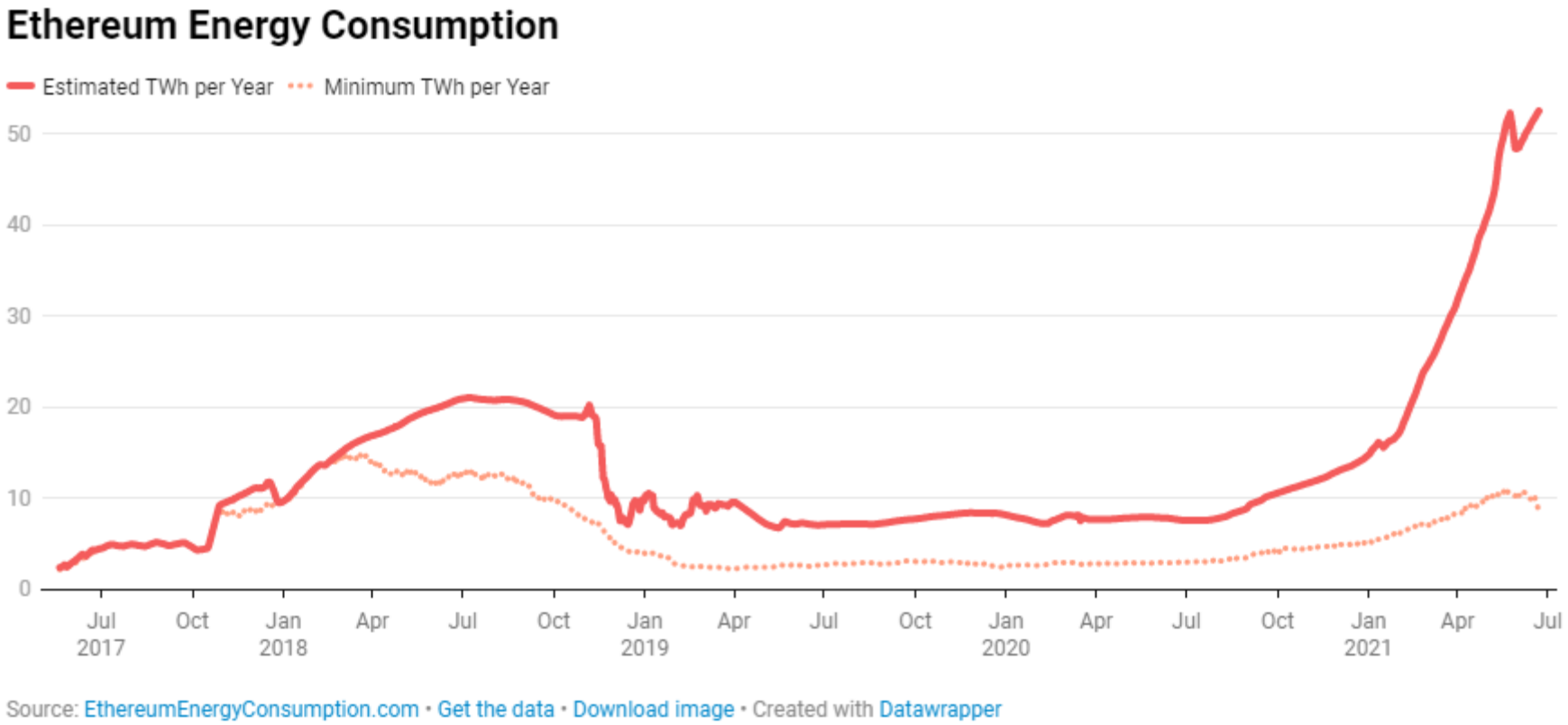
Bitcoin Energy Consumption Index

- https://digiconomist.net/bitcoin-energy-consumption



Ethereum Energy Consumption Index

- https://digiconomist.net/ethereum-energy-consumption



Single Transaction Footprints

Carbon Footprint

765.84 kgCO2

Equivalent to the carbon footprint of **1,697,368** VISA transactions or **127,640** hours of watching Youtube.

Electrical Energy

1612.30 kWh

Bitcoin

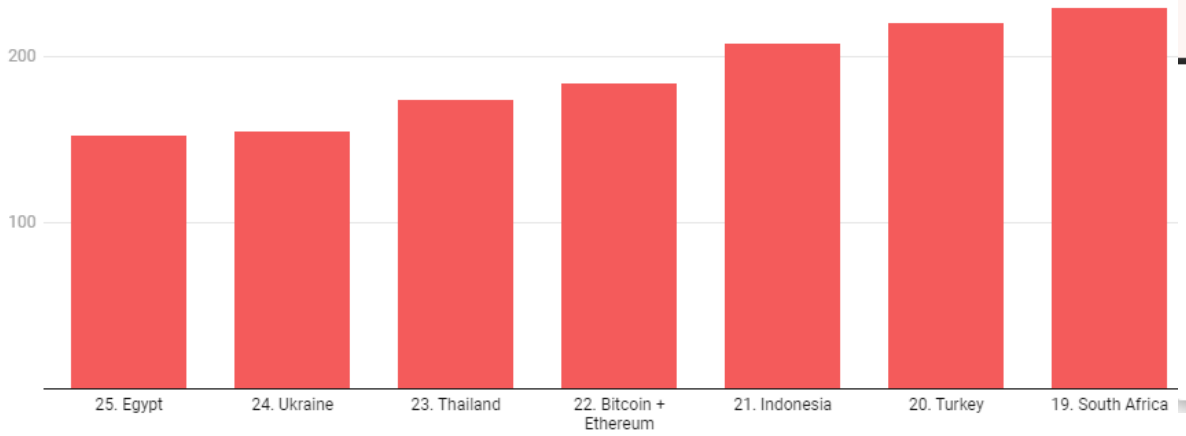
Equivalent to the power consumption of an average U.S. household over **55.26** days.

Electronic Waste

99.60 grams

Equivalent to the weight of **1.53** 'C'-size batteries or **2.17** golf balls. (Find more info on e-waste here.)

Energy Consumption by Country inc. Bitcoin + Ethereum (Annualized TWh)



Source: EthereumEnergyConsumption.com • Get the data • Download image • Created with Datawrapper

Electrical Energy

123.02 kWh

Ethereum

Equivalent to the power consumption of an average U.S. household over **4.16** days.

Proof of Stake

- The Proof of Stake (PoS) concept states that a person can mine or validate block transactions according to how many coins they hold.
- This means that the more coins owned by a miner, the more mining power they have.
- Comparing to Proof of Work (PoW)
  - Save energy?
  - ASIC vs. general computing
  - More resistant to attack? (From internal or external)
  - Fundamentally different from PoW?