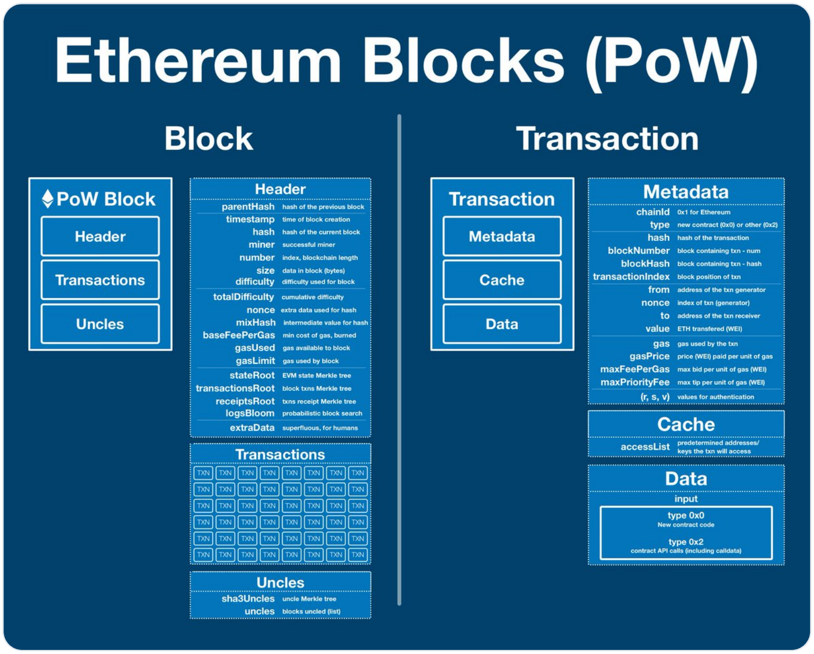
Haym Salomon @SalomonCrypto

Sep 9 · 19 tweets · SalomonCrypto/status/1568233231748841474

(1/18) @ethereum Fundamentals: PoW Blocks

Every ~15 seconds a new $ETH block is born... ever wondered what's inside?

A field-by-field guide to the building blocks that make up the blockchain.


Ethereum Blocks (PoW)
Block
Transaction
PoW Block
Header
Transactions
Uncles
Transaction
Metadata
Cache
Data
Header
Transactions
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
Uncles
Metadata
Cache
Data
input
type 0x0
New contract code
type 0x2
contract API calls (including calldata)

Header	
parentHash	hash of the previous block
timestamp	time of block creation
hash	hash of the current block
miner	successful miner
number	index, blockchain length
size	data in block (bytes)
difficulty	difficulty used for block
totalDifficulty	cumulative difficulty
nonce	extra data used for hash
mixHash	intermediate value for hash
baseFeePerGas	min cost of gas, burned
gasUsed	gas available to block
gasLimit	gas used by block
stateRoot	EVM state Merkle tree
transactionsRoot	block txns Merkle tree
receiptsRoot	txns receipt Merkle tree
logsBloom	probabilistic block search
extraData	superfluous, for humans

Uncles	
sha3Uncles	uncle Merkle tree
uncles	blocks uncled (list)

Metadata	
chainId	0x1 for Ethereum
type	new contract (0x0) or other (0x2)
hash	hash of the transaction
blockNumber	block containing txn - num
blockHash	block containing txn - hash
transactionIndex	block position of txn
from	address of the txn generator
nonce	index of txn (generator)
to	address of the txn receiver
value	ETH transfered (WEI)
gas	gas used by the txn
gasPrice	price (WEI) paid per unit of gas
maxFeePerGas	max bid per unit of gas (WEI)
maxPriorityFee	max tip per unit of gas (WEI)
(r, s, v)	values for authentication

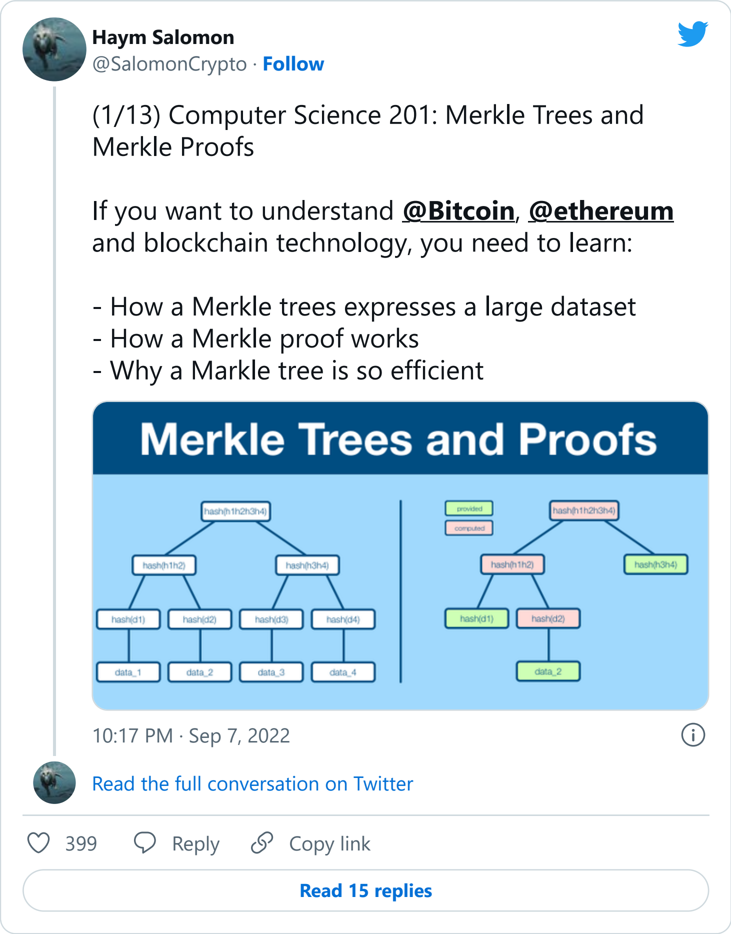
Cache	
accessList	predetermined addresses/ keys the txn will access

(2/18) @ethereum is the World Computer: a globally shared utility that exists between a network of 1000s of computers, each running a local version of the Ethereum Virtual Machine (EVM)

These nodes coordinate and sync their actions by building, proposing and distributing blocks

(3/18) Prerequisite - Merkle Trees

Merkle Tree: data structure used to organize and encrypt huge data sets. Merkle Proofs can be used to efficiently verify that data exists in a dataset (confirmation a piece of data exists without transferring the whole dataset).



Haym Salomon
@SalomonCrypto · **Follow**

(1/13) Computer Science 201: Merkle Trees and Merkle Proofs

If you want to understand **@Bitcoin**, **@ethereum** and blockchain technology, you need to learn:

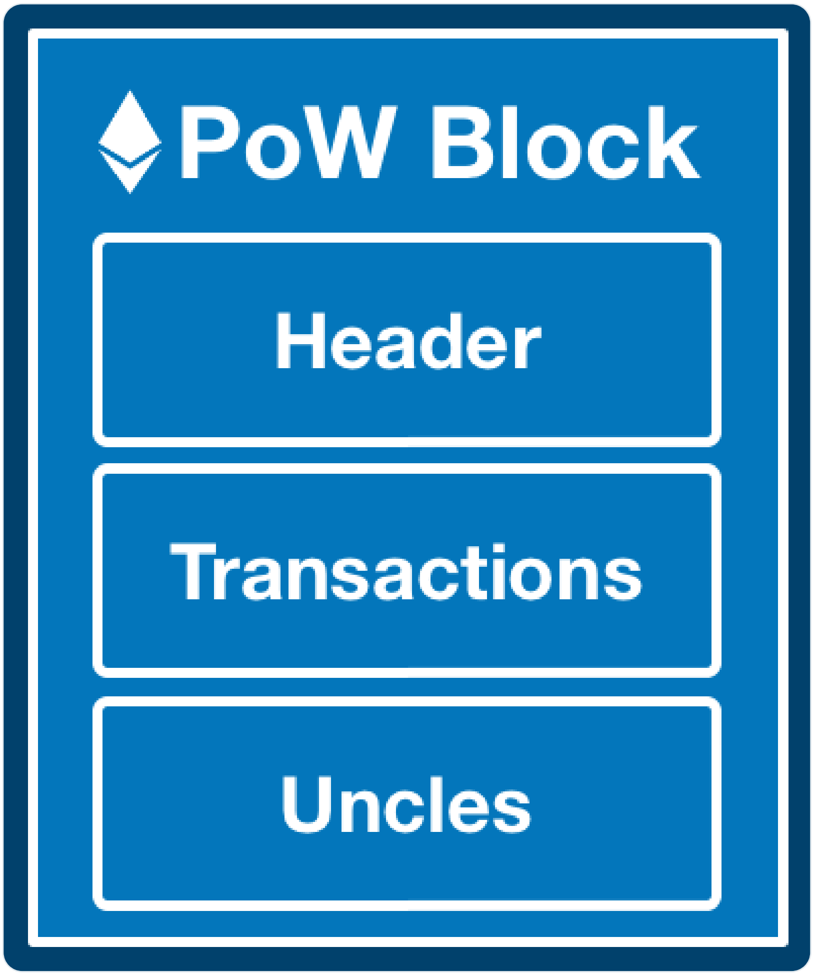
- How a Merkle trees expresses a large dataset
- How a Merkle proof works
- Why a Markle tree is so efficient

10:17 PM · Sep 7, 2022

Read the full conversation on Twitter

(4/18) An @ethereum block is made up of 3 parts:

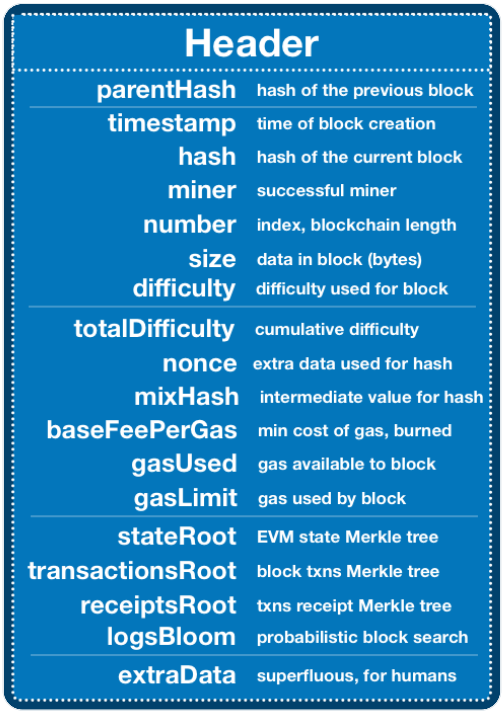
- Header, including all the metadata of the block
- Transactions, a list of all the transactions included in the block
- Uncles, management of uncles (a block that was broadcast simultaneously with another but not chosen)



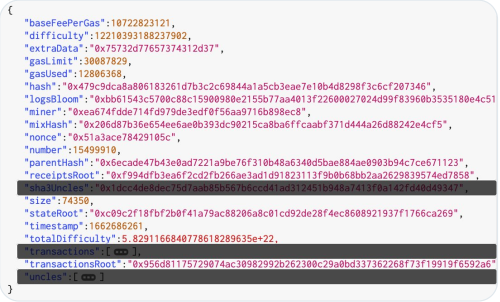
(5/18) Header - information about the block

The attached images show all the header fields. We will discuss the non-obvious ones in below.

timestamp - the date/time when the block was created, as reported by the block proposer



Header	
parentHash	hash of the previous block
timestamp	time of block creation
hash	hash of the current block
miner	successful miner
number	index, blockchain length
size	data in block (bytes)
difficulty	difficulty used for block
totalDifficulty	cumulative difficulty
nonce	extra data used for hash
mixHash	intermediate value for hash
baseFeePerGas	min cost of gas, burned
gasUsed	gas available to block
gasLimit	gas used by block
stateRoot	EVM state Merkle tree
transactionsRoot	block txns Merkle tree
receiptsRoot	txns receipt Merkle tree
logsBloom	probabilistic block search
extraData	superfluous, for humans



```
{
   "baseFeePerGas":10722823121,
   "difficulty":12210393188237902,
   "extraData":"0x75732d77657374312d37",
   "gasLimit":30087829,
   "gasUsed":12806368,
   "hash":"0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
   "logsBloom":"0xbb61543c5700c88c15900980e2155b77aa4013f22600027024d99f83960b3535180e4c51
   "miner":"0xea674fdde714fd979de3edf0f56aa9716b898ec8",
   "mixHash":"0x206d87b36e654ee6ae0b393dc90215ca8ba6ffcaabf371d444a26d88242e4cf5",
   "nonce":"0x51a3ace78429105c",
   "number":15499910,
   "parentHash":"0x6ecade47b43e0ad7221a9be76f310b48a6340d5bae884ae0903b94c7ce671123",
   "receiptsRoot":"0xf994dfb3ea6f2cd2fb266ae3ad1d91823113f9b0b68bb2aa2629839574ed7858",
   "sha3Uncles":"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
   "size":74350,
   "stateRoot":"0xc09c2f18fbf2b0f41a79ac88206a8c01cd92de28f4ec8608921937f1766ca269",
   "timestamp":1662686261,
   "totalDifficulty":5.829116684077861828963 5e+22,
   "transactions":[ ⋯ ],
   "transactionsRoot":"0x956d81175729074ac30982992b262300c29a0bd337362268f73f19919f6592a6"
   "uncles":[ ⋯ ]
}
```

(6/18) difficulty - a value that approximates the time a miner should calculate a hash function before finding a block. Network hash rate / difficulty = average block time

totalDifficulty - the cumulative value of the difficult required to build the chain up until this block

(7/18) nonce - extra data miners add to a block before hashing. A block is created when this hash matches a specific value; mining is the process of attempting to find this value by altering the nonce.

mixHash - intermediate value calculated from nonce, used for validation

(8/18) baseFeePerGas - EIP-1559 created a minimum cost (base fee) for each unit of gas. When a block is created, the entire base fee is burned. The value changes based on how full the previous block was (max change of 12.5% per block).

gasLimit - total gas available to the block

(9/18) stateRoot - the root hash of a Merkle tree which stores the entire state of the EVM (account balances, contract storage, contract code, etc)

transactionsRoot - the root hash of a Merkle tree which stores the transactions contained within the block.

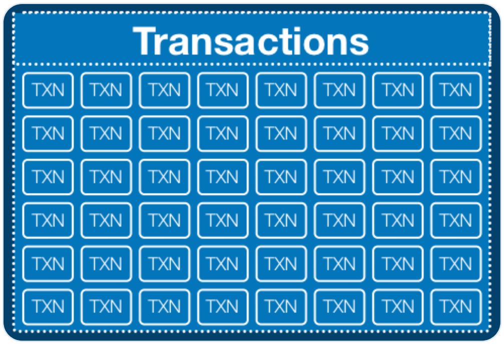
(10/18) receiptsRoot - the root hash of a Merkle tree which stores the receipts created by the transactions in a block. A receipt includes: block number, block hash, associated contracts, gas used, the stateRoot at the time (before) transaction, etc.

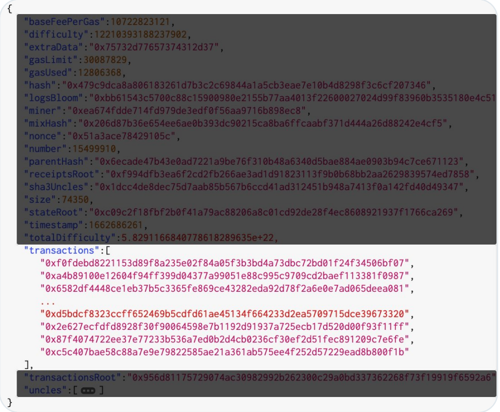
(11/18) logsBloom - a Bloom filter is a probabilistic structure that allows a user to filter through each element in the block. logsBloom minimize the number of queries a client needs to make.

https://llimllib.github.io/bloomfilter-tutorial/

(12/18) extraData - an (optional) 32-byte field in which block proposers can put anything they want. Often used by mining pools to log their blocks.

(13/18) Transactions - an ordered list of all the transactions executed within the block.


Transactions
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN
TXN TXN TXN TXN TXN TXN TXN TXN



```
{
  "baseFeePerGas":10722823121,
  "difficulty":12210393188237902,
  "extraData":"0x75732d77657374312d37",
  "gasLimit":30087829,
  "gasUsed":12806368,
  "hash":"0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
  "logsBloom":"0xbb61543c5700c88c15900980e2155b77aa4013f22600027024d99f83960b3535180e4c51
  "miner":"0xea674fdde714fd979de3edf0f56aa9716b898ec8",
  "mixHash":"0x206d87b36e654ee6ae0b393dc90215ca8ba6ffcaabf371d444a26d88242e4cf5",
  "nonce":"0x51a3ace78429105c",
  "number":15499910,
  "parentHash":"0x6ecade47b43e0ad7221a9be76f310b48a6340d5bae884ae0903b94c7ce671123",
  "receiptsRoot":"0xf994dfb3ea6f2cd2fb266ae3ad1d91823113f9b0b68bb2aa2629839574ed7858",
  "sha3Uncles":"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
  "size":74350,
  "stateRoot":"0xc09c2f18fbf2b0f41a79ac88206a8c01cd92de28f4ec8608921937f1766ca269",
  "timestamp":1662686261,
  "totalDifficulty":5.8291166840778618289635e+22,
  "transactions":[
     "0xf0fdebd8221153d89f8a235e02f84a05f3b3bd4a73dbc72bd01f24f34506bf07",
     "0xa4b89100e12604f94ff399d04377a99051e88c995c9709cd2baef113381f0987",
     "0x6582df4448ce1eb37b5c3365fe869ce43282eda92d78f2a6e0e7ad065deea081",
     ...
     "0xd5bdcf8323ccff652469b5cdfd61ae45134f664233d2ea5709715dce39673320",
     "0x2e627ecfdfd8928f30f90064598e7b1192d91937a725ecb17d520d00f93f11ff",
     "0x87f4074722ee37e77233b536a7ed0b2d4cb0236cf30ef2d51fec891209c7e6fe",
     "0xc5c407bae58c88a7e9e79822585ae21a361ab575ee4f252d57229ead8b800f1b"
  ],
  "transactionsRoot":"0x956d81175729074ac30982992b262300c29a0bd337362268f73f19919f6592a6
  "uncles":[ ... ]
}
```

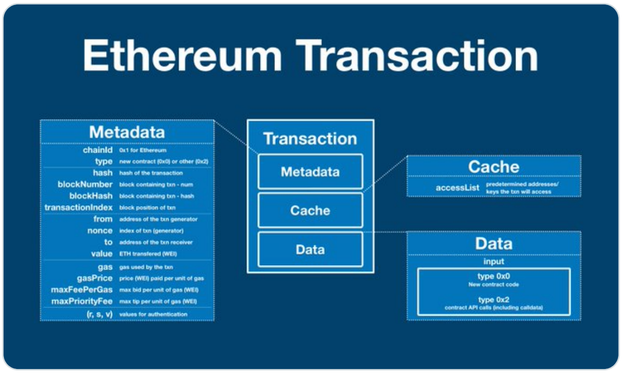
(14/18) For more information about the structure of @ethereum transactions, please see this thread:

Haym Salomon
@SalomonCrypto · **Follow**

(1/18) **@ethereum** Fundamentals: Transactions

Sent **$ETH**? LP'ed into an AMM? Deployed a new contract? Everything you do on the World Computer leaves an on-chain record. Ever wonder what's inside your transactions?

A field-by-field guide to the atomic unit of Ethereum computing



Ethereum Transaction

Metadata	
chainId	0x1 for Ethereum
type	new contract (0x0) or other (0x2)
hash	hash of the transaction
blockNumber	block containing txn - num
blockHash	block containing txn - hash
transactionIndex	block position of txn
from	address of the txn generator
nonce	index of txn (generator)
to	address of the txn receiver
value	ETH transfered (WEI)
gas	gas used by the txn
gasPrice	price (WEI) paid per unit of gas
maxFeePerGas	max bid per unit of gas (WEI)
maxPriorityFee	max tip per unit of gas (WEI)
(r, s, v)	values for authentication

Cache	
accessList	predetermined addresses/ keys the txn will access

Data
input
type 0x0
New contract code
type 0x2
contract API calls (including calldata)

4:22 AM · Sep 9, 2022

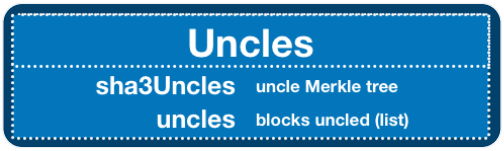
Read the full conversation on Twitter

279 Reply Copy link

Read 9 replies

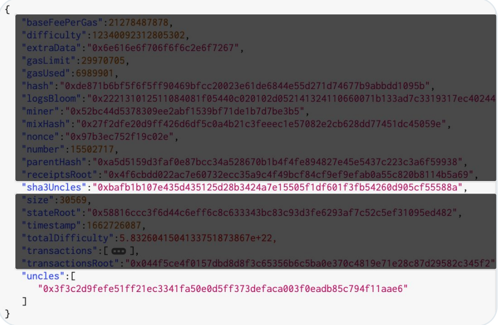
(15/18) Uncles - a list of the blocks "uncled" by this block.

Unless you're a core dev and/or battling in the MEV world, you can safely skip this subject for now.



Uncles

sha3Uncles	uncle Merkle tree
uncles	blocks uncled (list)



```
{
  "baseFeePerGas":21278487878,
  "difficulty":12340092312805302,
  "extraData":"0x6e616e6f706f6f6c2e6f7267",
  "gasLimit":29970705,
  "gasUsed":6989901,
  "hash":"0xde871b6bf5f6f5ff90469bfcc20023e61de6844e55d271d74677b9abbdd1095b",
  "logsBloom":"0x2221310125110840 81f05440c020102d0521413241106600 71b133ad7c3319317ec40244
  "miner":"0x52bc44d5378309ee2abf1539bf71de1b7d7be3b5",
  "mixHash":"0x27f2dfe20d9ff426d6df5c0a4b21c3feeec1e57082e2cb628dd77451dc45059e",
  "nonce":"0x97b3ec752f19c02e",
  "number":15502717,
  "parentHash":"0xa5d5159d3faf0e87bcc34a528670b1b4f4fe894827e45e5437c223c3a6f59938",
  "receiptsRoot":"0x4f6cbdd022ac7e60732ecc35a9c4f49bcf84cf9ef9efab0a55c820b8114b5a69",
  "sha3Uncles":"0xbafb1b107e435d435125d28b3424a7e15505f1df601f3fb54260d905cf55588a",
  "size":30569,
  "stateRoot":"0x58816ccc3f6d44c6eff6c8c633343bc83c93d3fe6293af7c52c5ef31095ed482",
  "timestamp":1662726087,
  "totalDifficulty":5.832604150413375187386 7e+22,
  "transactions":[ ••• ],
  "transactionsRoot":"0x044f5ce4f0157dbd8d8f3c65356b6c5ba0e370c4819e71e28c87d29582c345f2"
  "uncles":[
    "0x3f3c2d9fefe51ff21ec3341fa50e0d5ff373defaca003f0eadb85c794f11aae6"
  ]
}
```

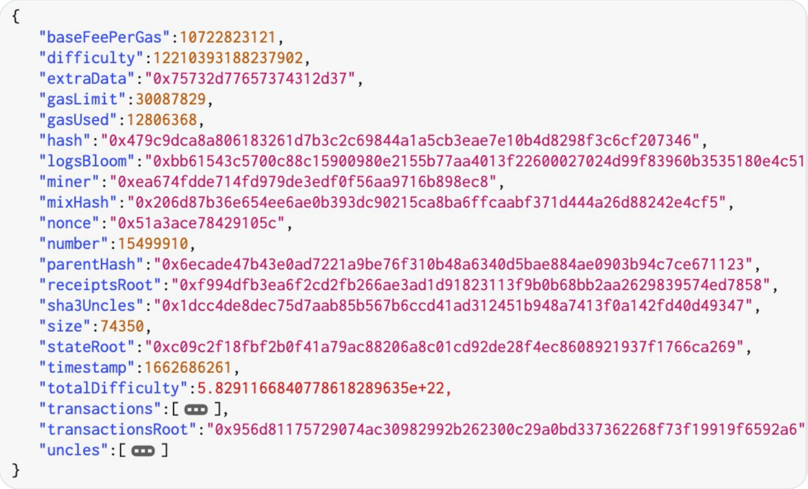
(16/18) Uncle blocks are created when 2 blocks are mined and sent to the network simultaneously. The block that gets validated by more nodes gets added to the blockchain.

The other block becomes an uncle block. Uncle blocks are recorded, but do not affect the EVM state.

(17/18) sha3Uncles - the root hash of a Merkle tree which stores all uncles for a given parent

uncles - a list of the blocks uncled by this block

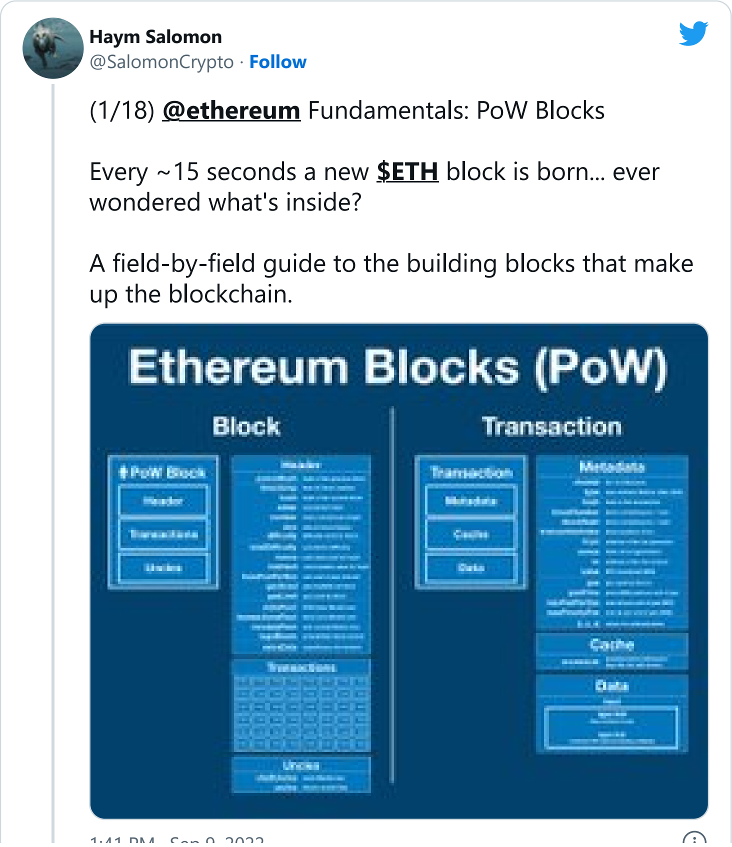
(18/18) And there you have it! That's an @ethereum (Proof of Work) block!



```
{
   "baseFeePerGas":10722823121,
   "difficulty":12210393188237902,
   "extraData":"0x75732d77657374312d37",
   "gasLimit":30087829,
   "gasUsed":12806368,
   "hash":"0x479c9dca8a806183261d7b3c2c69844a1a5cb3eae7e10b4d8298f3c6cf207346",
   "logsBloom":"0xbb61543c5700c88c15900980e2155b77aa4013f22600027024d99f83960b3535180e4c51
   "miner":"0xea674fdde714fd979de3edf0f56aa9716b898ec8",
   "mixHash":"0x206d87b36e654ee6ae0b393dc90215ca8ba6ffcaabf371d444a26d88242e4cf5",
   "nonce":"0x51a3ace78429105c",
   "number":15499910,
   "parentHash":"0x6ecade47b43e0ad7221a9be76f310b48a6340d5bae884ae0903b94c7ce671123",
   "receiptsRoot":"0xf994dfb3ea6f2cd2fb266ae3ad1d91823113f9b0b68bb2aa2629839574ed7858",
   "sha3Uncles":"0x1dcc4de8dec75d7aab85b567b6ccd41ad312451b948a7413f0a142fd40d49347",
   "size":74350,
   "stateRoot":"0xc09c2f18fbf2b0f41a79ac88206a8c01cd92de28f4ec8608921937f1766ca269",
   "timestamp":1662686261,
   "totalDifficulty":5.8291166840778618289635e+22,
   "transactions":[ … ],
   "transactionsRoot":"0x956d81175729074ac30982992b262300c29a0bd337362268f73f19919f6592a6"
   "uncles":[ … ]
}
```

Like what you read? Help me spread the word by retweeting the thread (linked below).

Follow me for more explainers and as much alpha as I can possibly serve.



Haym Salomon
@SalomonCrypto · Follow

(1/18) **@ethereum** Fundamentals: PoW Blocks

Every ~15 seconds a new **$ETH** block is born... ever wondered what's inside?

A field-by-field guide to the building blocks that make up the blockchain.

1:41 PM · Sep 9, 2022

• • •