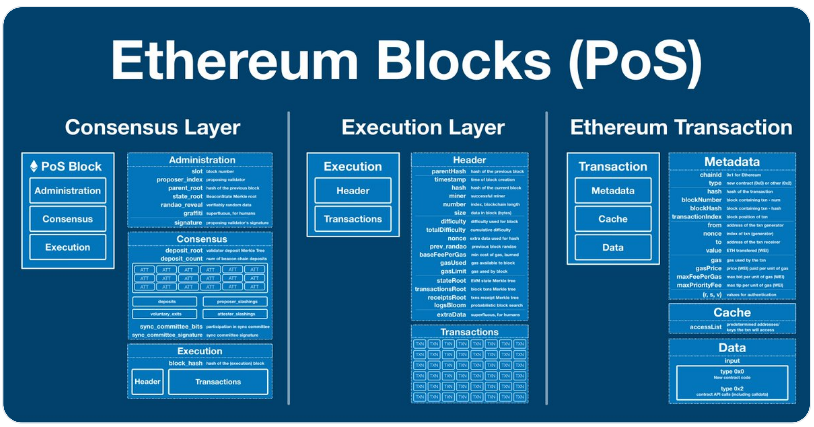
Haym Salomon @SalomonCrypto
Sep 9 · 22 tweets · SalomonCrypto/status/1568365818509139968

(1/21) @ethereum Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.

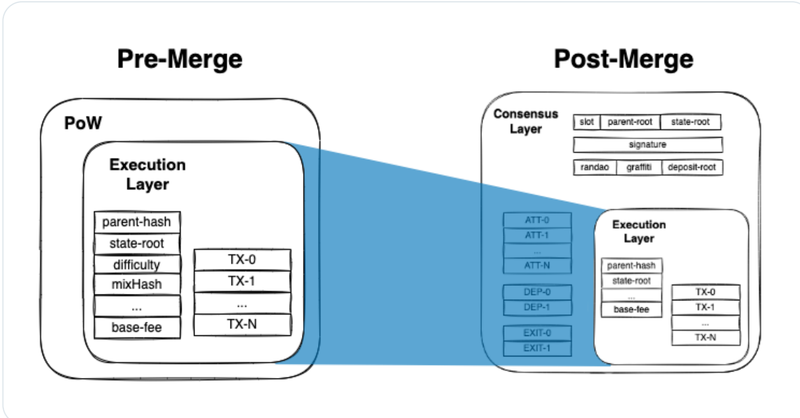


(2/21) @ethereum is the World Computer: a globally shared utility that exists between a network of 1000s of computers, each running a local version of the Ethereum Virtual Machine (EVM).

From genesis in 2015 until now, Ethereum has coordinated with a system called Proof of Work.

(3/21) In a few days, the @ethereum blockchain will Merge with the Beacon Chain, creating the new canonical PoS $ETH.

As the name "The Merge" suggests, Ethereum blocks will be a combination of the old blocks (execution layer) and the new Beacon Chain blocks (consensus layer).



(4/21) Prerequisite - Merkle Trees

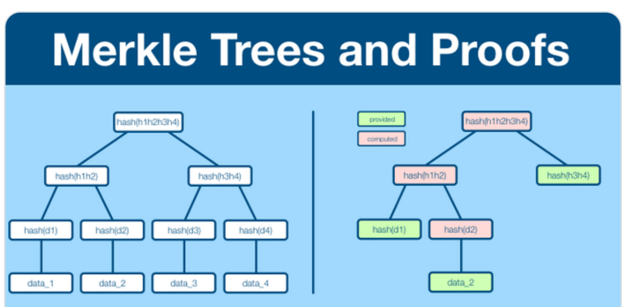
Merkle Tree: data structure used to organize and encrypt huge data sets. Merkle Proofs can be used to efficiently verify that data exists in a dataset (confirmation a piece of data exists without transferring the whole dataset).

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

399 Reply Copy link

Read 15 replies

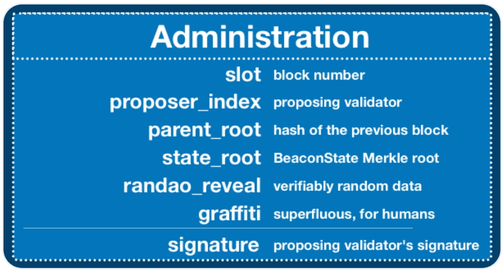
(5/21) Under PoS, an @ethereum block is made up of 3 parts:

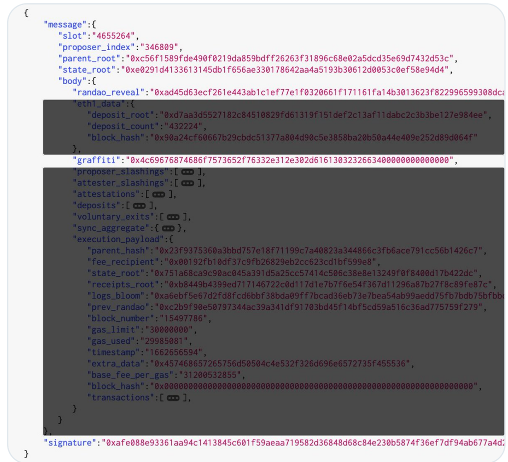
- Administration, the metadata of the block
- Consensus, the layer coordinating the Beacon Chain providing the cryptographic security of PoS
- Execution, the data of the block, (almost) exactly mirroring PoW blocks

(6/21) Administration - information about the block

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

state_root - the root hash of a Merkle tree which stores the state of the Beacon Chain (BeaconState)





(7/21) randao_reveal - protocol-verified randomness, generated between all block proposers during an epoch.

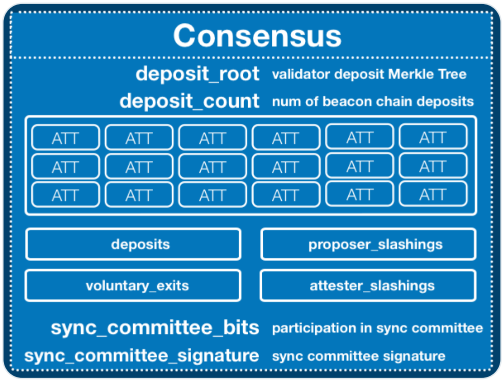
Randomness is critical to the Beacon Chain; security depends on being able to unpredictably and uniformly select block proposers and committee members.

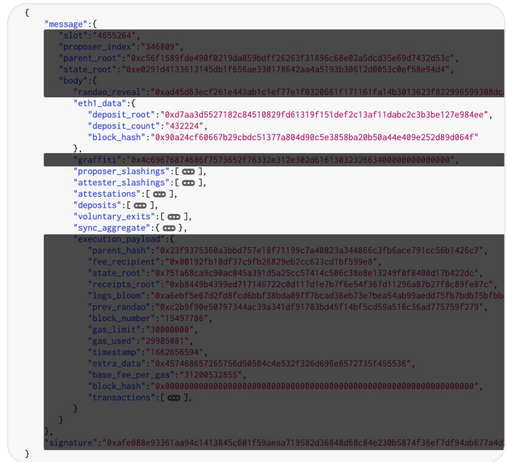
(8/21) graffiti - an (optional) 32-byte field in which block proposers can put anything they want. Often used by mining pools to log their blocks.

(9/21) signature - the signature the block proposer creates to take responsibility (add to blockchain and collect reward if good, get slashed if bad). Created by combining the BeaconState, BeaconBlock and the proposer's private key.

(10/21) Consensus - information necessary to coordinate and verify blockchain consensus and implement PoS

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



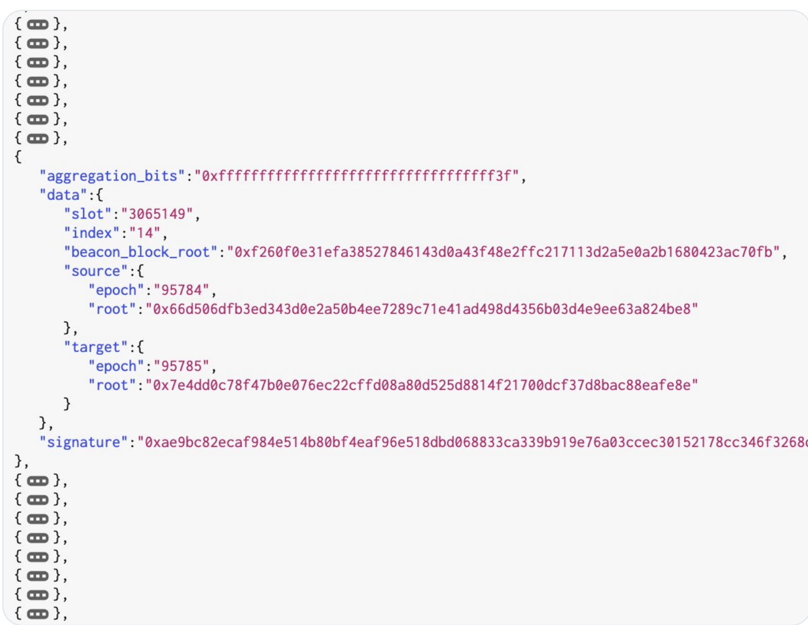


(11/21)deposit_root - the root hash of a Merkle tree which stores the $ETH deposits into the staking contract (required to become a validator)

attestations - a list of all validators that attested to this block

(12/21) [@ethereum](https://twitter.com/ethereum) PoS elects a proposer who is charged with building (or selecting) a block and proposing it to the network. Attesters review the block and, if it's valid, sign it with their keys.

attestations - a list of these signatures, represented in this data structure:



```
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{
   "aggregation_bits":"0xffffffffffffffffffffffffffffffff3f",
   "data":{
      "slot":"3065149",
      "index":"14",
      "beacon_block_root":"0xf260f0e31efa38527846143d0a43f48e2ffc217113d2a5e0a2b1680423ac70fb",
      "source":{
         "epoch":"95784",
         "root":"0x66d506dfb3ed343d0e2a50b4ee7289c71e41ad498d4356b03d4e9ee63a824be8"
      },
      "target":{
         "epoch":"95785",
         "root":"0x7e4dd0c78f47b0e076ec22cffd08a80d525d8814f21700dcf37d8bac88eafe8e"
      }
   },
   "signature":"0xae9bc82ecaf984e514b80bf4eaf96e518dbd068833ca339b919e76a03ccec30152178cc346f3268c
},
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
{ ... },
```

(13/21) deposits - @beaconcha_in defines this field as "amount of validator deposits which have been included in this block by the block proposer." Interestingly, the only non-0 value I could find was in the genesis block

voluntary_exits - withdrawals from the staking contract

(14/21) proposer_slashings and attester_slashings - validators that have performed a hostile action against the network (for example, proposing or attesting to an invalid block). The network confiscates a portion of their staked $ETH and ejects them from the validator set.


```
"proposer_slashings":[

],
"attester_slashings":[
  {
    "attestation_1":{
      "attesting_indices":[ ... ],
      "data":{
        "slot":"3065149",
        "index":"41",
        "beacon_block_root":"0xf260f0e31efa38527846143d0a43f48e2ffc217113d2a5e0a2b1680423ac70fb",
        "source":{
          "epoch":"95784",
          "root":"0x66d506dfb3ed343d0e2a50b4ee7289c71e41ad498d4356b03d4e9ee63a824be8"
        },
        "target":{
          "epoch":"95785",
          "root":"0x7e4dd0c78f47b0e076ec22cffd08a80d525d8814f21700dcf37d8bac88eafe8e"
        }
      },
      "signature":"0x97cb1bb5937a2a73e6f4c7c723a26639fe805a66dca20be57cfe2cb50952198dad07970b80bb9b66b
    },
    "attestation_2":{
      "attesting_indices":[ ... ],
      "data":{
        "slot":"3065149",
        "index":"41",
        "beacon_block_root":"0xdecc2c104369b2bdd93c6fdbe6370ab1fdfb9c51d391c9dd76a1a3e6816dd4f5",
        "source":{
          "epoch":"95784",
          "root":"0x66d506dfb3ed343d0e2a50b4ee7289c71e41ad498d4356b03d4e9ee63a824be8"
        },
        "target":{
          "epoch":"95785",
          "root":"0x7e4dd0c78f47b0e076ec22cffd08a80d525d8814f21700dcf37d8bac88eafe8e"
        }
      },
      "signature":"0x87e116e34f6736c3a9350e127e9cb82b9977cfba49acc71ea208e7af6181982e84e305e3ef89c8fec
    }
  }
],
```

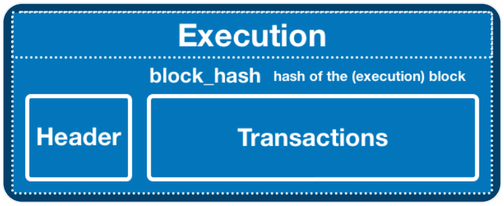

(15/21) A sync committee is a group of 512 validators, randomly assigned once every 256 epochs (~27 hours). This committee creates the signatures needed for an efficient light client.

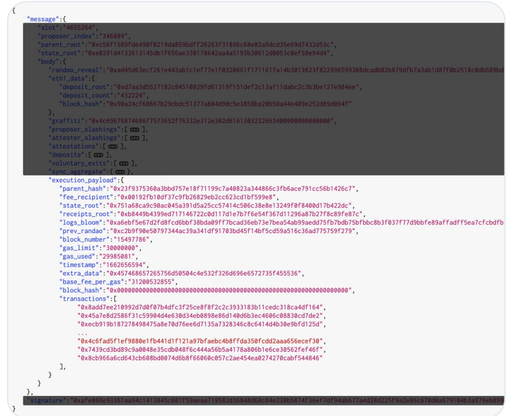
(16/21) sync_committee_bits - efficient representation of committee participation

sync_committee_signature - the signature the sync committee creates to take responsibility for the block/epoch

(17/21) Execution - the payload of the @ethereum block, including all transaction data.

The attached images show all the execution fields.





(18/21) For many purposes (particularly backwards compatibility), the execution payload of a PoS block looks almost identical to a PoW block. For more information, please see this thread.

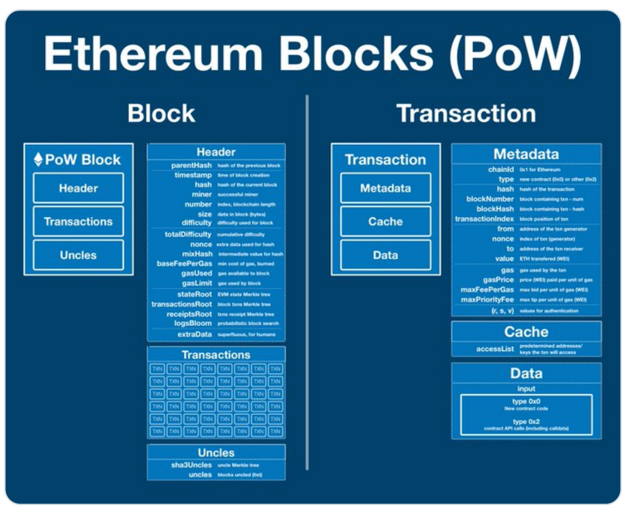
We will cover the (minor) changes below.

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

Read the full conversation on Twitter

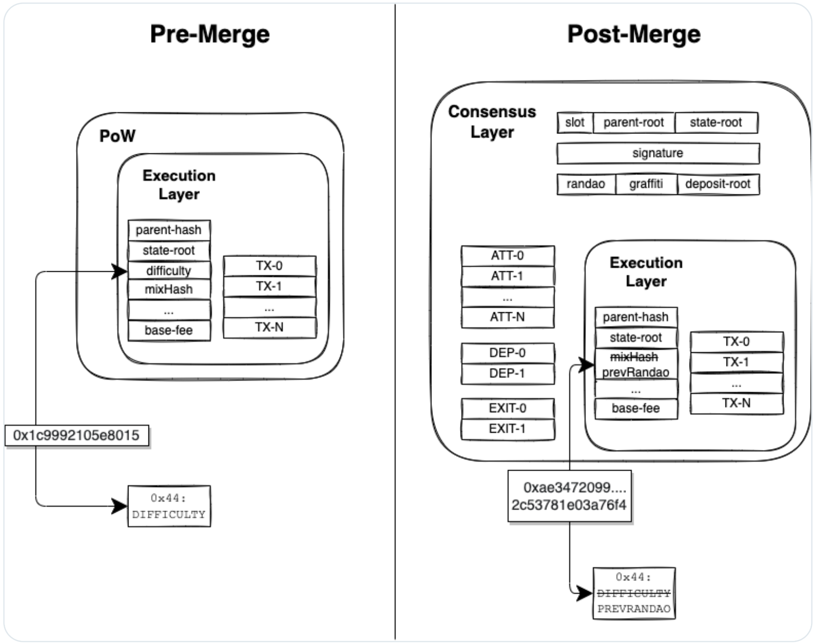
85 Reply Copy link

Read 2 replies

(19/21) difficulty - set to 0 (PoS does not have difficulty)

nonce - set to 0x0000000000000000 (PoS does not use a nonce)

mixHash - has been renamed to prev_randao now stores the randao value from the previous block



(20/21) sha3Uncles and uncles - because proof of stake does not naturally produce uncle blocks, these fields will be set to 0 (or the hash of an empty list in the case of sha3Uncles). These fields have become irrelevant.

(21/21) And there you have it! That's an [@ethereum](https://twitter.com/ethereum) (Proof of Stake) block!


```
{
    "message":{
      "slot":"4655264",
      "proposer_index":"346809",
      "parent_root":"0xc56f1589fde490f0219da859bdff26263f31896c68e02a5dcd35e69d7432d53c",
      "state_root":"0xe0291d4133613145db1f656ae330178642aa4a5193b30612d0053c0ef58e94d4",
      "body":{
        "randao_reveal":"0xad45d63ecf261e443ab1c1ef77e1f0320661f171161fa14b3013623f822996599308dcadb02b879dfb7a3ab1d87f0b2518c0db689bd
        "eth1_data":{
          "deposit_root":"0xd7aa3d5527182c84510829fd61319f151def2c13af11dabc2c3b3be127e984ee",
          "deposit_count":"432224",
          "block_hash":"0x90a24cf60667b29cbdc51377a804d90c5e3858ba20b50a44e409e252d89d064f"
        },
        "graffiti":"0x4c69676874686f7573652f76332e312e302d6161303232663400000000000000",
        "proposer_slashings":[ ••• ],
        "attester_slashings":[ ••• ],
        "attestations":[ ••• ],
        "deposits":[ ••• ],
        "voluntary_exits":[ ••• ],
        "sync_aggregate":{ ••• },
        "execution_payload":{
          "parent_hash":"0x23f9375360a3bbd757e18f71199c7a40823a344866c3fb6ace791cc56b1426c7",
          "fee_recipient":"0x00192fb10df37c9fb26829eb2cc623cd1bf599e8",
          "state_root":"0x751a68ca9c90ac045a391d5a25cc57414c506c38e8e13249f0f8400d17b422dc",
          "receipts_root":"0xb8449b4399ed717146722c0d117d1e7b7f6e54f367d11296a87b27f8c89fe87c",
          "logs_bloom":"0xa6ebf5e67d2fd8fcd6bbf38bda09ff7bcad36eb73e7bea54ab99aedd75fb7bdb75bfbbc8b3f037f77d9bbfe89affadff5ea7cfcbdfb
          "prev_randao":"0xc2b9f90e50797344ac39a341df91703bd45f14bf5cd59a516c36ad775759f279",
          "block_number":"15497786",
          "gas_limit":"30000000",
          "gas_used":"29985081",
          "timestamp":"1662656594",
          "extra_data":"0x457468657265756d50504c4e532f326d696e6572735f455536",
          "base_fee_per_gas":"31200532855",
          "block_hash":"0x0000000000000000000000000000000000000000000000000000000000000000",
          "transactions":[
              "0x8add7ee210992d7d0f07b4dfc3f25ce8f8f2c2c3933183b11cedc318ca4df164",
              "0x45a7e8d2586f31c59904d4e630d34eb0898e86d140d6b3ec4606c08830cd7de2",
              "0xecb919b187278498475a8e70d76ee6d7135a7328346c8c6414d4b30e9bfd125d",
              ...,
              "0x4c6fad5f1ef9880e1fb441d1f121a97bfaebc4b8ffda350fcdd2aaa656ecef30",
              "0x7439cd3bd89c9a0048e35cdb048f6c444a56b5a4178a806b1e6ce30562fef46f",
              "0x8cb966a6cd643cb608bd0074d6b8f66060c057c2ae454ea0274270cabf544846"
          ],
        }
      }
    },
    "signature":"0xafe088e93361aa94c1413845c601f59aeaa719582d36848d68c84e230b5874f36ef7df94ab677a4d28d225f9a2e86c670d0a679104b3a976eb899
}
```

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

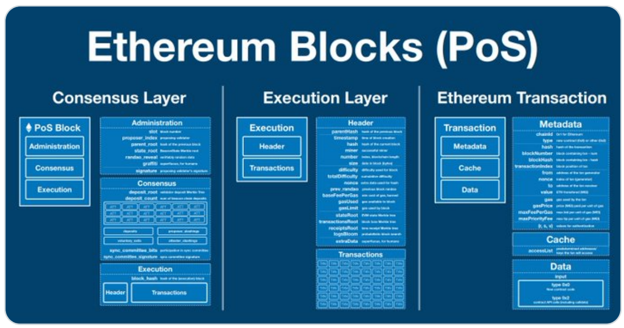
Follow me for more explainers and as much alpha as I can possibly serve.

Haym Salomon
@SalomonCrypto · **Follow**

(1/21) **@ethereum** Fundamentals: PoS Blocks

In less than 1 week, the Ethereum blockchain will Merge with the Beacon Chain and the World Computer will transition from PoW to PoS. The blockchain will never be the same.

A field-by-field guide to on-chain future.



10:28 PM · Sep 9, 2022

Read the full conversation on Twitter

58 Reply Copy link

Read 6 replies

• • •