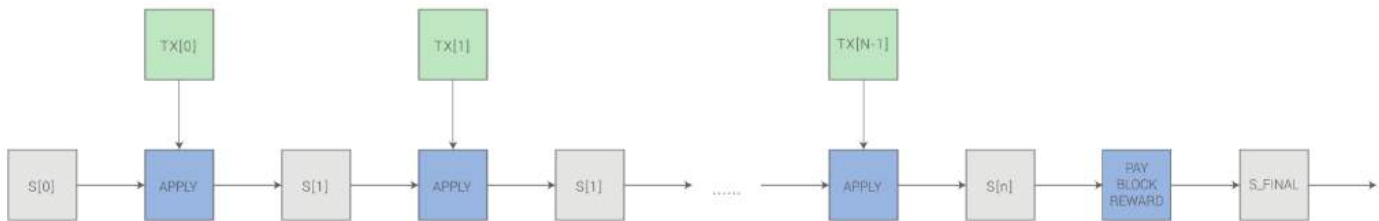


## Blockchain and Mining



The Ethereum blockchain is in many ways similar to the Bitcoin blockchain, although it does have some differences. The main difference between Ethereum and Bitcoin with regard to the blockchain architecture is that, unlike Bitcoin, Ethereum blocks contain a copy of both the transaction list and the most recent state. Aside from that, two other values, the block number and the difficulty, are also stored in the block. The block validation algorithm in Ethereum is as follows:

1. Check if the previous block referenced exists and is valid.
2. Check that the timestamp of the block is greater than that of the referenced previous block and less than 15 minutes into the future
3. Check that the block number, difficulty, transaction root, uncle root and gas limit (various low-level Ethereum-specific concepts) are valid.
4. Check that the proof of work on the block is valid.
5. Let  $S[0]$  be the `STATE_ROOT` of the previous block.
6. Let  $TX$  be the block's transaction list, with  $n$  transactions. For all  $i$  in  $0 \dots n-1$ , set  $S[i+1] = \text{APPLY}(S[i], TX[i])$ . If any application returns an error, or if the total gas consumed in the block up until this point exceeds the `GASLIMIT`, return an error.
7. Let  $S\_FINAL$  be  $S[n]$ , but adding the block reward paid to the miner.
8. Check if  $S\_FINAL$  is the same as the `STATE_ROOT`. If it is, the block is valid; otherwise, it is not valid.

