Proof of Capacity (PoC)

Anthony Tam & Michael O'Connell

Distributed Ledger

Distributed Ledger

- A ledger is a collection of transactions within the network
- A transaction is the transfer of funds from a sender to a recipient
- A copy of the ledger is maintained by every node in the network, so that no one node can decide what transactions are included in the ledger
- Additionally, all transactions added must be verified by the sender

Proof of Work

Proof of Work

- In order to solidify a segment of the ledger into the record, you have to form a block
- A block is a list of transactions which have occured on the network
- In order to create a block, a member of the network must find a string which, when hashed with the list of transactions, contains a particular prefix; this string is called the “Proof of Work”

Proof of Work

- This “Proof of Work” is then verified by the other nodes in the network, at which point they then add it to their copies of the ledger
- As an additional security measure, the block also begins with the hash of the previous block, which ensures that no blocks have been maliciously inserted, removed, or altered by any other nodes on the network

Proof of Capacity

Proof of Capacity

- Created in 2015
- Instead of computational power, storage capacity is used
- First, a few requirements

A Plot

- A file containing pre-computed hashes
- Used to generate blocks in the blockchain
- Many plots are created for each device mining

Hash Function

- A one way function
- Typically a slower hash function is used for PoC
- This makes the hash results important to save, rather then attempt to recompute them for each block
- Functions such as Shabal or Cryptonote are prefered, rather then SHA or Scrypt
- Typically with a 256 bit output length

Nonce Values

- A value which is only used once per miner
- A number between 0 and 2^64
- This value is used alot with the wallet to seed the hash function
- Each nonce value used contains 256KB of hashes

Scoop

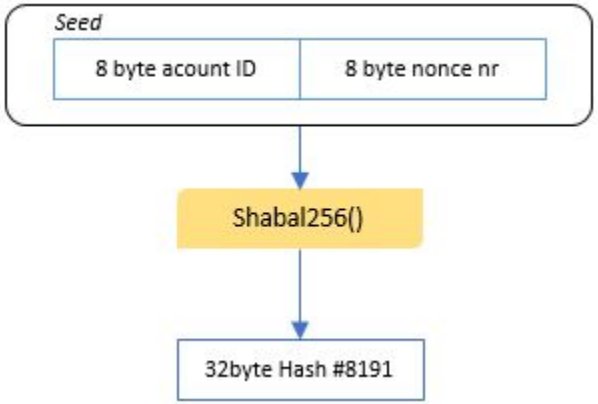
- Each nonce contains 256KB, or 8192 hashes
- Each hash is paired and stored in a 64 byte scoop
- These scoops will be important for the mining process as they are directly referenced

Plotting

- Creating plots on the specified storage device

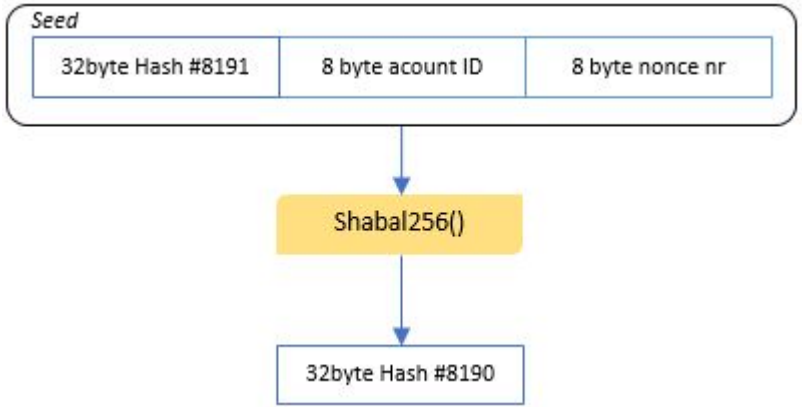
Plotting Process

- Create a 16 byte seed by concatenating an 8 byte wallet ID with an 8 byte nonce value
- Hash this seed with your hash function
- This has is the last hash in this nonce set



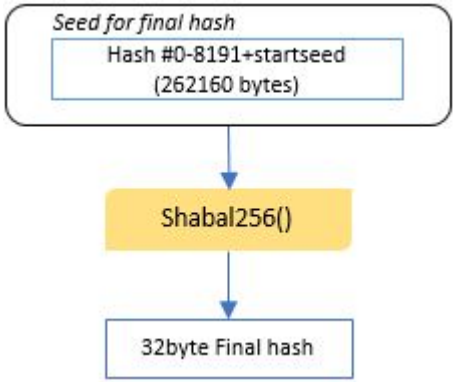
Plotting Process

- The previous hash is the appended to the original seed
- The hash function is run again on this new seed
- This process is repeated until the seed reaches 4096 bytes
- Once this occurs, only the latest 4096 bytes are used



Plotting Process

- Once all hashes are created, a final hash is generated
- This is seeded by all 8192 hash values and the original start seed
- All other hash values are then XOR'ed to this final hash

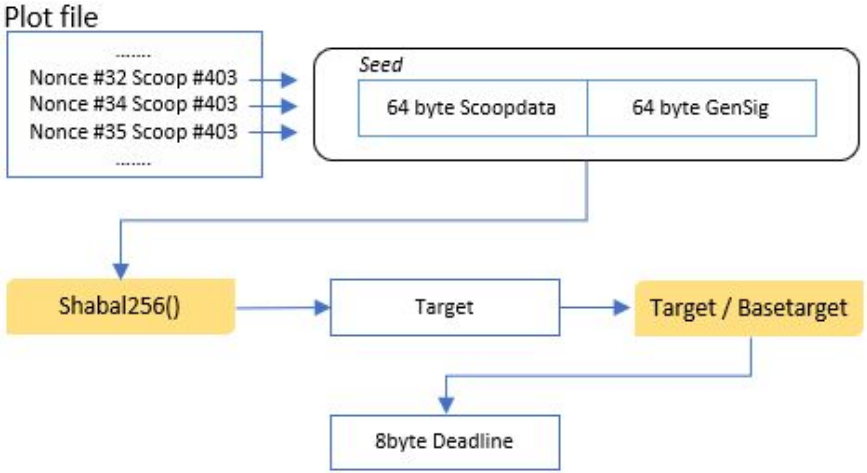


Mining

- Firstly, a miner must create the signature of the block they are attempting to create
- This signature must take into account the previous block to form a chain
- The previous generation signature and the account which found the last block are concatenated together and hashed
- This hash is then concatenated to the new block height and hashed again, known as the generation signature
- This generation signature is then modulo 4096, the result is a scoop number

Mining

- Each 64 byte scoop is concatenated to the generation signature and hashed
- This hash is divided by the network difficulty
- The first 8 bytes of this quotient is known as the deadline
- The deadline represents the number of seconds until the miner creates a block, assuming there is no smaller deadline on the network



Mining

- When a deadline is submitted to the network, the nonce value and wallet ID are also submitted, signed by the wallets private key (Digital Signature)
- This allows a node on the network the verify this wallet did generate this deadline

Pros & Cons

Pros

- Aside from plotting, very little computational power is used
- Once a storage device is plotted, mining only consists of lookups on the drive
- Generally, storage capacity is far more economical and reusable then GPU’s/ASIC miners
- When the user no longer wishes to mine, the drives can be repurposed since they have gone through very few write cycles


WHAT
IS
BURST

Cons

- Plotting is a very slow process
- Using average hardware, it takes approximately 5 days to plot 400GB
- There are not many implementations of proof of capacity and therefore has not been rigorously tested
- When storage is plotted, it cannot be used for anything else

A Demo

References

- https://burstwiki.org/wiki/Technical_information_to_create_plot_files
- https://burstwiki.org/wiki/Technical_information_about_mining_and_block_forging
- https://coincentral.com/what-is-proof-of-capacity/