AuxPoW and mining

Hey everybody,

in this article I will describe what auxiliary Proof of Work is, using Dogecoin as currency. I will also explain all technical terms to keep it beginner friendly.

Auxiliary Proof of Work, or AuxPoW, means that the proof of work can be provided by **another chain**. For Dogecoin the parent chain[1] is Litecoin.

To understand this, we need to know what **proof of work** is and which purpose it serves.

A crypto currency is a **decentralized network** with peer to peer connections. This means there is no central server providing information, but a network of clients sharing all information. A client can be a Dogecoin Core wallet[2]. Those wallets are also referred as nodes. They have a copy of the blockchain and check and propagate all valid data.

To have **consensus**[3] of which transactions have happened so far, the chain needs to sequentialize the transactions into blocks[4]. Only transactions in at least one block „have happened". A new block gets propagated every minute. The time is defined in the block time[5]. And it can contain one to a lot of transactions[6]. It has to contain at least one transaction and that is the coinbase transaction[7], sending the mining reward to its miner. This reward is also called block reward and contains the newly generated coins that are added to the total supply of coins. This is the incentive for the miner to do the work. For Dogecoin it is 10,000 Dogecoins per block.

All transactions propagated, that are not in a block yet, will be stored in the mempool[8] until they are in a block or would drop out again, i.e. when they had insufficient fees in their transaction.

So you may wonder, what is **mining**[9]. To answer this, we need to understand which purpose mining serves. It needs to be expensive to create consensus to prevent nodes submitting new blocks immediately, because we want to sequentialize the transactions. The currency can do this by demanding to **solve an issue**.

People often say the miner needs to solve a cryptographic puzzle to find a block. But what they actually do is to find the **nonce**[10]. The nonce is a number that is one of many input parameters that is send into a hash function.

Hash functions[11] are calculations that are applied to data. In our example a bit later, we will have two strings as input into the hash function. You can't predict the resulting hash value based on the input strings. If you change the string even a bit, the hash value will change completely. However, the hash function is deterministic. This means it will always have the same hash value for the same inputs.

In mining, most input strings are given, like the previous block hash. That's why it is called **block chain**, because the blocks are linked.

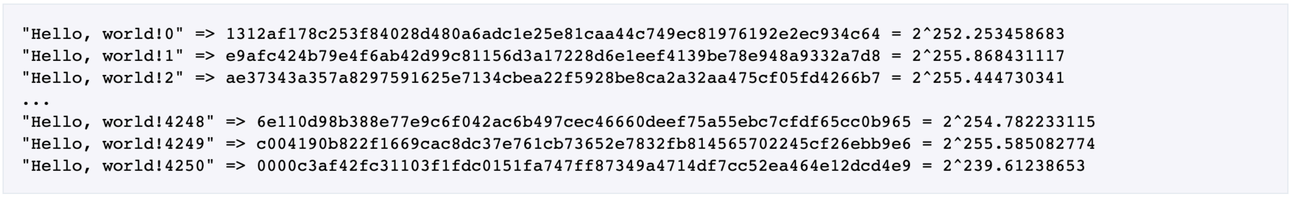
If you are wondering why the chain uses block hashes and not the block number, check orphaned blocks[12] - same number, different hashes!

Back to the inputs! One input isn't given - it is the **nonce**, the number that needs be added as input to the hash function and will change the hash value completely. The network will **only accept** the hash of the block **if it is smaller than the target**[13]. This defines the **difficulty**. The difficulty can be converted to a hex number with leading zeros and the miners try to find a hash value that is smaller than the target. Due to the fact that the miner can't predict the hash value, they have to try different nonce values as input over and over again. The tries per second i.e. of a miner are described as hashes per second[14].

The higher the difficulty, the more leading zeroes you need in your hash value, or the smaller the hash value needs to be.

The **proof of work is** the fact that a miner **found the nonce**.

A great way to demonstrate this is by the following example based on the screenshot from bitcoin.it. We only accept the block hash if it has four leading zeroes. We want to have two input streams, the string „Hello, world!“ and our nonce. It would take 4251 tries to find a nonce if we start with zero and increment by one until we get a hash that contains four leading zeros:



```
"Hello, world!0" => 1312af178c253f84028d480a6adc1e25e81caa44c749ec81976192e2ec934c64 = 2^252.253458683
"Hello, world!1" => e9afc424b79e4f6ab42d99c81156d3a17228d6e1eef4139be78e948a9332a7d8 = 2^255.868431117
"Hello, world!2" => ae37343a357a8297591625e7134cbea22f5928be8ca2a32aa475cf05fd4266b7 = 2^255.444730341
...
"Hello, world!4248" => 6e110d98b388e77e9c6f042ac6b497cec46660deef75a55ebc7cfdf65cc0b965 = 2^254.782233115
"Hello, world!4249" => c004190b822f1669cac8dc37e761cb73652e7832fb814565702245cf26ebb9e6 = 2^255.585082774
"Hello, world!4250" => 0000c3af42fc31103f1fdc0151fa747ff87349a4714df7cc52ea464e12dcd4e9 = 2^239.61238653
```

Source: bitcoin.it[15]

The network knows its current hash rate of all miners. Therefore it can calculate the amount of hashing tries the network can perform per second and how many seconds it should take until the next block will be found. Therefore it can set the difficulty to a value to stay at the same block time even if the hash rates increases or drops.

If we can make 100 hashes per second and want to have a block every 60 seconds we want to create a difficulty where we expect 60 * 100 tries until we find a fitting nonce.

The miner can decide which transactions should be added to the block. Usually he will use the transactions based on the fees the sender added to his transaction. This will be added to the miners reward for „finding the block“.

After we understand this, we can finally have a look on the „**auxiliary**“ part of the document.

An AuxPoW currency like Dogecoin is merged mined. This means the LTC miners will apply their work to LTC - the parent chain - and Dogecoin - the auxiliary blockchain - when the miner participates in **merged mining**. A miner only mining LTC with no merged mining wouldn’t benefit from the additional Dogecoin block rewards and Dogecoin wouldn’t benefit from the additional hash rate securing the network. However both currencies could still be mined on their own.

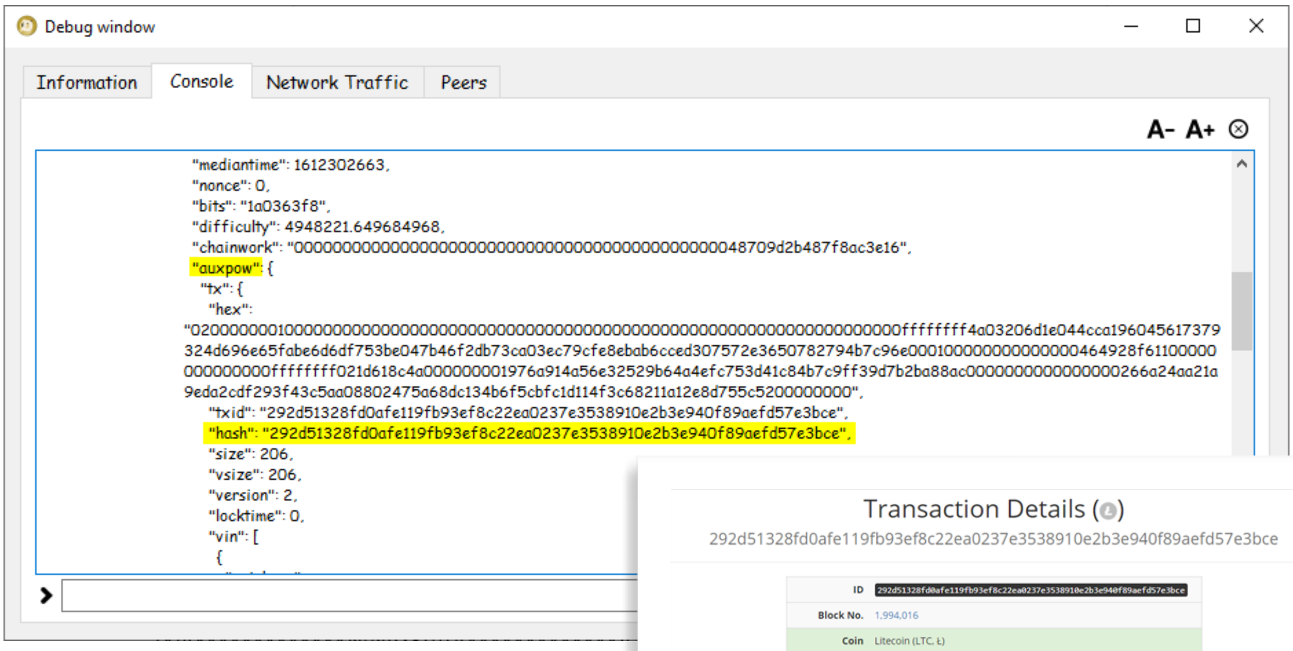
If a LTC miner is trying to find the correct nonce for LTC, he may not find an accepted one for LTC, but could find a nonce creating a suitable hash for Dogecoin.

See this example:

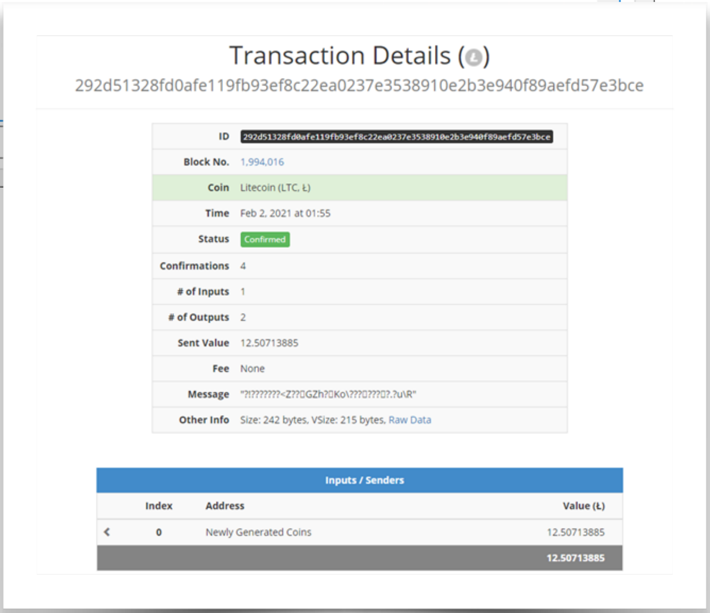
Miner	**Litecoin**	**Dogecoin**
	Has a block time of 2.5, therefore a high difficulty	Has a bock time of 1, therefore a smaller difficulty
	Difficulty 000100	Difficulty 001000
Finds nonce that generates hash 000900	✗	✓
Finds nonce that generates hash 000090	✓	✓

Dogecoin blocks will reference the Litecoin blockchain. We will only be able to find the referenced hash if the miner found a nonce that generates a block hash that is small enough for both chains. If it is only valid on Dogechain the parent chain will refuse the hash and you won't be able to find the hash on the parent chain.

If the nonce created a valid hash for **both chains** can will display that reference in the Dogecoin blockchain and the reference it the LTC blockchain like this:



```
        "mediantime": 1612302663,
        "nonce": 0,
        "bits": "1a0363f8",
        "difficulty": 4948221.649684968,
        "chainwork": "000000000000000000000000000000000000000000000048709d2b487f8ac3e16",
        "auxpow": {
          "tx": {
            "hex":
"02000000010000000000000000000000000000000000000000000000000000000000000000ffffffff4a03206d1e044cca196045617379
324d696e65fabe6d6df753be047b46f2db73ca03ec79cfe8ebab6cced307572e3650782794b7c96e0001000000000000000464928f61100000
00000000ffffffff021d618c4a000000001976a914a56e32529b64a4efc753d41c84b7c9ff39d7b2ba88ac0000000000000000266a24aa21a
9eda2cdf293f43c5aa08802475a68dc134b6f5cbfc1d114f3c68211a12e8d755c5200000000",
            "txid": "292d51328fd0afe119fb93ef8c22ea0237e3538910e2b3e940f89aefd57e3bce",
            "hash": "292d51328fd0afe119fb93ef8c22ea0237e3538910e2b3e940f89aefd57e3bce",
            "size": 206,
            "vsize": 206,
            "version": 2,
            "locktime": 0,
            "vin": [
              {
```



Transaction Details

292d51328fd0afe119fb93ef8c22ea0237e3538910e2b3e940f89aefd57e3bce

ID	292d51328fd0afe119fb93ef8c22ea0237e3538910e2b3e940f89aefd57e3bce
Block No.	1,994,016
Coin	Litecoin (LTC, Ł)
Time	Feb 2, 2021 at 01:55
Status	Confirmed
Confirmations	4
# of Inputs	1
# of Outputs	2
Sent Value	12.50713885
Fee	None
Message	"?!???????<Z??GZh?Ko\???????.?u\R"
Other Info	Size: 242 bytes, VSize: 215 bytes, Raw Data

Inputs / Senders

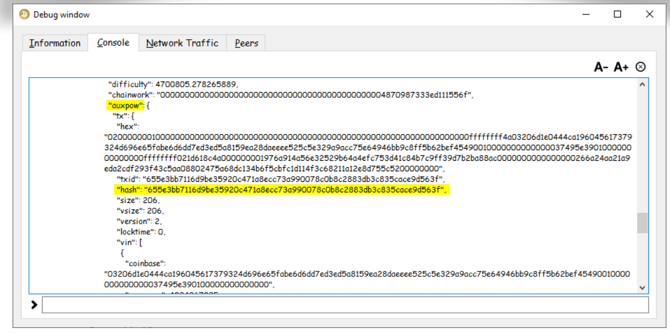
	Index	Address	Value (Ł)
<	0	Newly Generated Coins	12.50713885
			12.50713885

In the screenshot above we can see the reference hash of the Litecoin blockchain. If we search for that hash we will find the coinbase transaction, or block reward of Dogecoins parent chain (LTC).

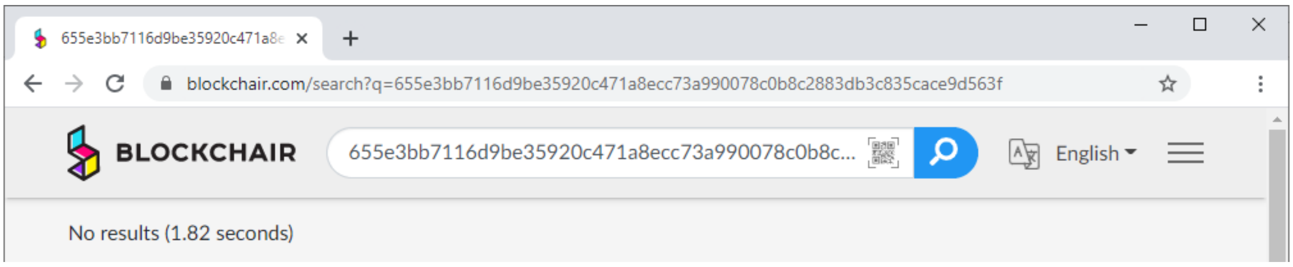
Transaction ID:
`292d51328fd0afe119fb93ef8c22ea02`
`37e3538910e2b3e940f89aefd57e3bce`

But you could also find a nonce generating a hash that is small enough for Dogecoin but not small enough for Litecoin. Therefore the hash wasn't accepted by the Litecoin network and you won't find the Litecoin block hash:

Transaction ID:
`655e3bb7116d9be35920c471a8ecc73a`
`990078c0b8c2883db3c835cace9d563f`



```
        "difficulty": 4700805.278265889,
        "chainwork": "000000000000000000000000000000000000000000004870987333ed111556f",
        "auxpow": {
          "tx": {
            "hex":
"02000000010000000000000000000000000000000000000000000000000000000000000000ffffffff4a03206d1e0444ca196045617379
324d696e65fabe6d6dd7ed3ed5a8159ea28daeeee525c5e329a9acc75e64946bb9c8ff5b62bef4549001000000000000037495e3901000000
00000000ffffffff021d618c4a000000001976a914a56e32529b64a4efc753d41c84b7c9ff39d7b2ba88ac0000000000000000266a24aa21a9
eda2cdf293f43c5aa08802475a68dc134b6f5cbfc1d114f3c68211a12e8d755c5200000000",
            "txid": "655e3bb7116d9be35920c471a8ecc73a990078c0b8c2883db3c835cace9d563f",
            "hash": "655e3bb7116d9be35920c471a8ecc73a990078c0b8c2883db3c835cace9d563f",
            "size": 206,
            "vsize": 206,
            "version": 2,
            "locktime": 0,
            "vin": [
              {
                "coinbase":
"03206d1e0444ca196045617379324d696e65fabe6d6dd7ed3ed5a8159ea28daeeee525c5e329a9acc75e64946bb9c8ff5b62bef45490010000
000000000037495e3901000000000000000",
```


655e3bb7116d9be35920c471a8e
blockchair.com/search?q=655e3bb7116d9be35920c471a8ecc73a990078c0b8c2883db3c835cace9d563f
BLOCKCHAIR
655e3bb7116d9be35920c471a8ecc73a990078c0b8c...
English

No results (1.82 seconds)

With the two given block times we should find five Dogecoin blocks in five minutes, and two Litecoin blocks if every Litecoin miner would be merged mining. Therefore we should have three Dogecoin blocks referencing a Litecoin block hash we will not be able to find on the Litecoin blockchain in those five minutes.

You could also find a Dogecoin block with no „AuxPoW“ information in it. In this case you would have a Dogecoin block that wasn’t merged mined. This is still possible, however from a profit perspective it won’t make a lot of sense for most miners.

Conclusion: Merged mining is a great incentive for miners, because the work will be applied to two chains instead of only one at almost no extra costs. LTC doesn’t have any drawbacks and Dogecoin is secured by Litecoins great hash rate if the miners take advantage of merged mining.

This is why Dogecoin still secure, not easy to mine and my very favorite coin.

If you enjoyed this read so much you want to throw your money at me, feel free to send a tip to this address:
`DAuxPoWHaPGZm1i5xgsHVKBBpZdE7LPNiB`

If you have any question, may ask on www.reddit.com/r/dogecoin

Thank you for reading this article and special thanks to everybody supported me to create this roundup.

Best regards,

nformant

Sources:
1 https://en.bitcoin.it/wiki/Merged_mining_specification#Terminology (Dogecoins parent chain could be any scrypt chain! This was just simplified)
2 https://en.bitcoin.it/wiki/Full_node
3 https://en.bitcoin.it/wiki/Consensus
4 https://en.bitcoin.it/wiki/Block
5 https://en.wikipedia.org/wiki/Dogecoin
6 https://www.reddit.com/r/dogecoin/comments/2w62zh/technical_question_about_transaction_size/
7 https://en.bitcoin.it/wiki/Coinbase
8 https://www.blockchain.com/en/charts/mempool-size?timespan=all
9 https://en.bitcoin.it/wiki/Mining
10 https://en.bitcoin.it/wiki/Nonce
11 https://en.bitcoin.it/wiki/Hash
12 https://www.investopedia.com/terms/o/orphan-block-cryptocurrency.asp
13 https://en.bitcoin.it/wiki/Target
14 https://en.bitcoin.it/wiki/Hash_per_second
15 https://en.bitcoin.it/wiki/Proof_of_work#Example

Graphical sources:
All icons from: www.flaticon.com
Credit to the icon authors:
Becris: https://creativemarket.com/Becris
Good Ware: ttps://www.flaticon.com/authors/good-ware
Smashicons: https://www.flaticon.com/authors/smashicons
smalllikeart: https://www.flaticon.com/authors/smalllikeart
Freepik: https://www.freepik.com
Kiranshastry: https://www.flaticon.com/authors/kiranshastry
Prosymbols: https://www.flaticon.com/authors/prosymbols

Font (sig.): https://creativemarket.com/typeline