XDAG: algorithm of mining

## Introduction

Each 64 seconds each pool generates a new block. One of these blocks which has a hash with the highest difficulty become the man block. The lower hash of block the higher its difficulty.

Block has a field - nonce. This field is has integer type. The purpose of mining is to find a value for nonce which allows to generate minimal hash for block. Pool does not perform searching the value for nonce itself, but it allows miners to connect and find a nonce. So pool generates new task each 64 seconds and sends it to miners. And each miner tries to find a value for nonce which allows to generate block with the lowest hast and sends the nonces back to pool as shares.

Share has size of 32 bytes. Each share consists of two parts:

* Low 24 bytes of hash of miners address.
* 8-bytes nonce.

Pool processes received shares and saves the one which allows to generate the lowest hash for the new block.

There is no target difficulty as in other cryptocurrencies, like bitcoin. Mining continues until current interval of time (64 second) is ended. Then pool generates a new block with the best share, sends it to network and creates task for mining for a new block. When pool generate a new block, whole share is written in the last field of the block.

## Examples

### Miner has founded minimal hash, pool generated a new block based on received share

2018-07-20 22:48:18.434 [000002cf9de0:INFO] Task : t=16d48f2ffff N=2

2018-07-20 22:48:24.434 [000002cf9de0:INFO] Share : 000000b7410fe824c7858b02d95dd3362d8813216ce0a9bb874e495159cb74f9 t=16d48f2ffff res=0

2018-07-20 22:48:34.434 [000002cf9de0:INFO] Share : 00000045062d6c334e171233a6c870763cbd7ec7e9162fdc314836f6d6879c2b t=16d48f2ffff res=0

2018-07-20 22:48:44.443 [000002cf9de0:INFO] Share : **0000000b804806ca39161a7db06e4b8f94d5dd3797d2d4fac1b0498622e9e13f** t=16d48f2ffff res=0

xdag> block 0000000b804806ca39161a7db06e4b8f94d5dd3797d2d4fac1b0498622e9e13f

time: 2018-07-20 22:49:19.999

timestamp: 16d48f2ffff

flags: 1f

state: Main

file pos: 0

hash: **0000000b804806ca39161a7db06e4b8f94d5dd3797d2d4fac1b0498622e9e13f**

difficulty: 374e9fe95f0de1a98bee4

balance: P+HpIoZJsMH61NKXN93VlI9LbrB9GhY5 10.239999999

-------------------------------------------------------------------------------------------

block as transaction: details

direction address amount

-------------------------------------------------------------------------------------------

fee: P+HpIoZJsMH61NKXN93VlI9LbrB9GhY5 0.000000000

output: pkMmN35uEkZfrUNi/unaQoPwgkKbvetu 0.000000000

output: pkMmN35uEkZfrUNi/unaQoPwgkKbvetu 0.000000000

-------------------------------------------------------------------------------------------

block as address: details

direction transaction amount time

-------------------------------------------------------------------------------------------

earning: P+HpIoZJsMH61NKXN93VlI9LbrB9GhY5 1024.000000000 2018-07-20 22:49:19.999

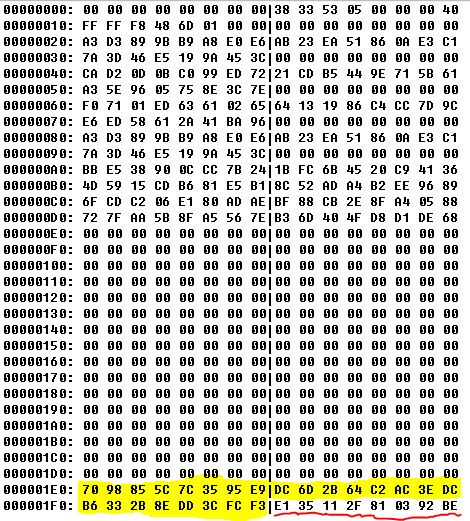
output: iaO8JUPyquZbfZKiFE0dePAy2HLYQCi1 1013.760000000 2018-07-20 23:04:17.970

### Share as a part of the block

Hash of address:

d4c4015dee6e3b8cf3fc3cdd8e2b33b6dc3eacc2642b6ddce995357c5c859870

Hexadecimal representation of mined block:



Highlighted part is low 24 bytes of hash of address in little-endian representation:

f3 fc 3c dd 8e 2b 33 b6 dc 3e ac c2 64 2b 6d dc e9 95 35 7c 5c 85 98 70

Underlined part is a nonce.

## 

## Technical side

Pool pays for blocks which were mined 960 seconds ago (15 intervals \* 64 seconds). So network has enough time to synchronize and choose the main block.

Pool stores best shares for each miner for the last 16 tasks. There is array with 16 items:

| 0 | 1 | 2 | 3 | 4 | 5 | 6 | 7 | 8 | 9 | 10 | 11 | 12 | 13 | 14 | 15 |

Each item represents interval with duration 64 seconds.

When interval is started - a new task is sent to all miners. During that interval all miners send shares for that task. When the interval is ended - a block is generated based on the most difficult share and sent to network. After it the next interval is started. The processing is cyclic - when 15-th interval is ended index is set to 0.

Payments are done based on block mined 15 intervals ago. It means if current interval is 15, payments are processed for block mined at interval №0. If that block didn't become main - pool has nothing to pay. Next payment process will be done in the next interval.

If block created at interval №0 became main - the process of payments is started. Pool takes current earning (1024 XDAG), subtracts all fees and then calculates the payments.

If there is no rewards for miner who mined a block and for direct contribution, the formula of payment is: share - share rate for current miner in interval № X sum - sum of shares from all miners in the interval № X payment = (1024 - fees) \* share / sum