DogeChia Whitepaper

Abstract

This document describes the principles and approach of the DogeChia blockchain. In consideration of the technology created by Bram Cohen, namely Proof of Space and Time (PoST), it considers the mechanism of co-farming Chia plots while describing the rationale for the existence of the DogeChia fork.

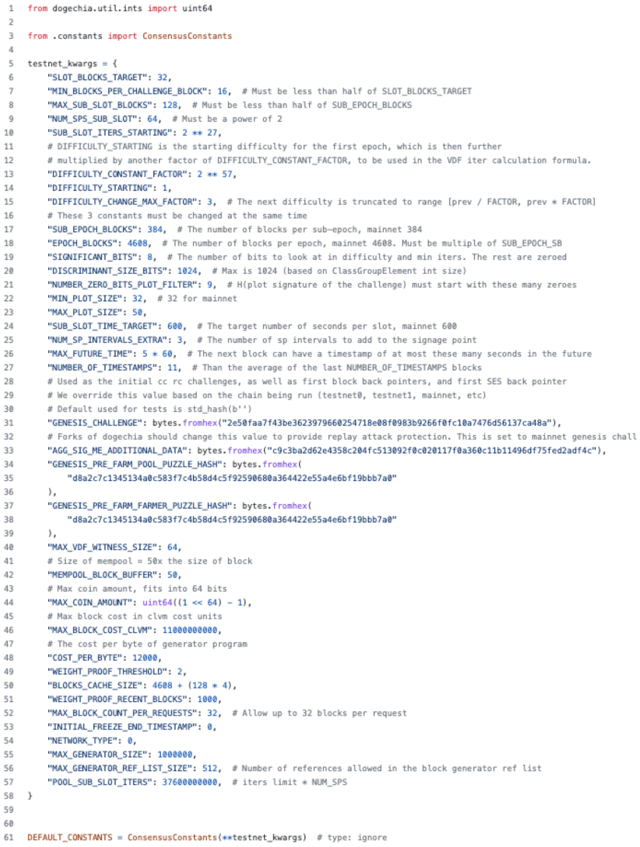
DogeChia

The early days of Bitcoin realized various forks of the codebased providing minor if any variation on the originally published source. History repeats with a variety of Chia blockchain forks arising in the summer of 2021.

These Chia forks offer almost no differentiation from Chia other than a search and replace change of the name Chia to a different project name. Inherently this is not entirely bad as the full operation of a Chia fork requires more than forking the codebase and making a few changes. The project team needs ensure that Timelords are properly running to ensure the chain will continue to advance, Introducers are configured properly to ensure that farmers and full nodes can connect to peers, and that changes in farming techniques (such as NFT plots) are responded by updating project source or consensus as necessary. By undertaking the above, a project demonstrates its value.

The community of Chia fork farmers believes in the inherent value of the DogeChia blockchain, voting with their attention to co-farming. It has been consistently referenced as one of the most well run chains with respect to reliability and consistency.[1,2]

The DogeChia blockchain stayed abreast of early developments in the Chia ecosystem adopting the 1.2.x Chia codebase changes containing NFT plot code days after release[3], demonstrating the team's cability to keep pace with important developments in the Chia ecosystem.

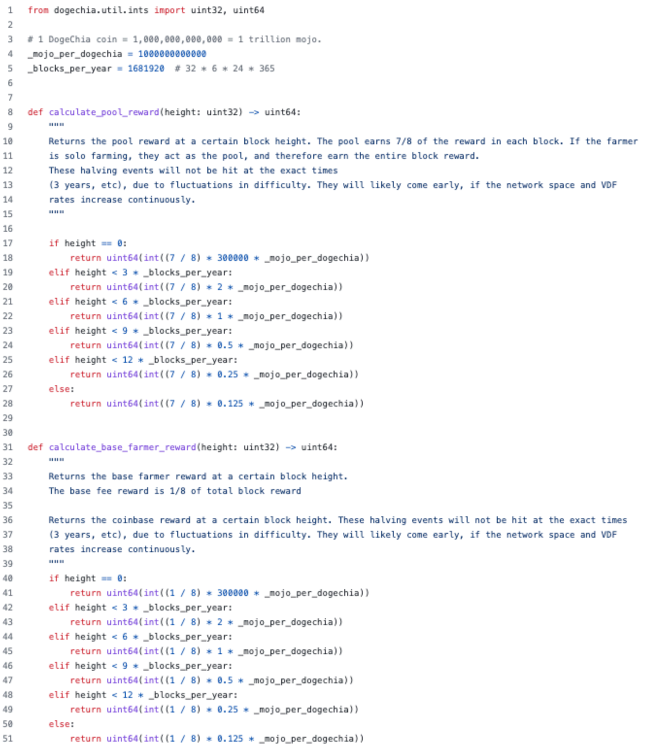


```python
from dogechia.util.ints import uint64

from .constants import ConsensusConstants

testnet_kwargs = {
    "SLOT_BLOCKS_TARGET": 32,
    "MIN_BLOCKS_PER_CHALLENGE_BLOCK": 16,  # Must be less than half of SLOT_BLOCKS_TARGET
    "MAX_SUB_SLOT_BLOCKS": 128,  # Must be less than half of SUB_EPOCH_BLOCKS
    "NUM_SPS_SUB_SLOT": 64,  # Must be a power of 2
    "SUB_SLOT_ITERS_STARTING": 2 ** 27,
    # DIFFICULTY_STARTING is the starting difficulty for the first epoch, which is then further
    # multiplied by another factor of DIFFICULTY_CONSTANT_FACTOR, to be used in the VDF iter calculation formula.
    "DIFFICULTY_CONSTANT_FACTOR": 2 ** 57,
    "DIFFICULTY_STARTING": 1,
    "DIFFICULTY_CHANGE_MAX_FACTOR": 3,  # The next difficulty is truncated to range [prev / FACTOR, prev * FACTOR]
    # These 3 constants must be changed at the same time
    "SUB_EPOCH_BLOCKS": 384,  # The number of blocks per sub-epoch, mainnet 384
    "EPOCH_BLOCKS": 4608,  # The number of blocks per epoch, mainnet 4608. Must be multiple of SUB_EPOCH_SB
    "SIGNIFICANT_BITS": 8,  # The number of bits to look at in difficulty and min iters. The rest are zeroed
    "DISCRIMINANT_SIZE_BITS": 1024,  # Max is 1024 (based on ClassGroupElement int size)
    "NUMBER_ZERO_BITS_PLOT_FILTER": 9,  # H(plot signature of the challenge) must start with these many zeroes
    "MIN_PLOT_SIZE": 32,  # 32 for mainnet
    "MAX_PLOT_SIZE": 50,
    "SUB_SLOT_TIME_TARGET": 600,  # The target number of seconds per slot, mainnet 600
    "NUM_SP_INTERVALS_EXTRA": 3,  # The number of sp intervals to add to the signage point
    "MAX_FUTURE_TIME": 5 * 60,  # The next block can have a timestamp of at most these many seconds in the future
    "NUMBER_OF_TIMESTAMPS": 11,  # Than the average of the last NUMBER_OF_TIMESTAMPS blocks
    # Used as the initial cc rc challenges, as well as first block back pointers, and first SES back pointer
    # We override this value based on the chain being run (testnet0, testnet1, mainnet, etc)
    # Default used for tests is std_hash(b'')
    "GENESIS_CHALLENGE": bytes.fromhex("2e50faa7f43be3623979660254718e08f0983b9266f0fc10a7476d56137ca48a"),
    # Forks of dogechia should change this value to provide replay attack protection. This is set to mainnet genesis chall
    "AGG_SIG_ME_ADDITIONAL_DATA": bytes.fromhex("c9c3ba2d62e4358c204fc513092f0c020117f0a360c11b11496df75fed2adf4c"),
    "GENESIS_PRE_FARM_POOL_PUZZLE_HASH": bytes.fromhex(
        "d8a2c7c1345134a0c583f7c4b58d4c5f92590680a364422e55a4e6bf19bbb7a0"
    ),
    "GENESIS_PRE_FARM_FARMER_PUZZLE_HASH": bytes.fromhex(
        "d8a2c7c1345134a0c583f7c4b58d4c5f92590680a364422e55a4e6bf19bbb7a0"
    ),
    "MAX_VDF_WITNESS_SIZE": 64,
    # Size of mempool = 50x the size of block
    "MEMPOOL_BLOCK_BUFFER": 50,
    # Max coin amount, fits into 64 bits
    "MAX_COIN_AMOUNT": uint64((1 << 64) - 1),
    # Max block cost in clvm cost units
    "MAX_BLOCK_COST_CLVM": 11000000000,
    # The cost per byte of generator program
    "COST_PER_BYTE": 12000,
    "WEIGHT_PROOF_THRESHOLD": 2,
    "BLOCKS_CACHE_SIZE": 4608 + (128 * 4),
    "WEIGHT_PROOF_RECENT_BLOCKS": 1000,
    "MAX_BLOCK_COUNT_PER_REQUESTS": 32,  # Allow up to 32 blocks per request
    "INITIAL_FREEZE_END_TIMESTAMP": 0,
    "NETWORK_TYPE": 0,
    "MAX_GENERATOR_SIZE": 1000000,
    "MAX_GENERATOR_REF_LIST_SIZE": 512,  # Number of references allowed in the block generator ref list
    "POOL_SUB_SLOT_ITERS": 37600000000,  # iters limit * NUM_SPS
}


DEFAULT_CONSTANTS = ConsensusConstants(**testnet_kwargs)  # type: ignore
```

Figure 1: doge-chia/dogechia/consensus/default_constants.py

1.1 Technical Details

DogeChia is technically a fork of the Flax blockchain which itself is a fork of the Chia blockchain[4]. To achieve technical differentiation from each of these projects DogeChia modified two files **default_constants.py**[5] and **block_rewards.py**[6] in the **doge-chia/dogechia/consensus** folder of the blockchain repository.



```python
 1  from dogechia.util.ints import uint32, uint64
 2
 3  # 1 DogeChia coin = 1,000,000,000,000 = 1 trillion mojo.
 4  _mojo_per_dogechia = 1000000000000
 5  _blocks_per_year = 1681920  # 32 * 6 * 24 * 365
 6
 7
 8  def calculate_pool_reward(height: uint32) -> uint64:
 9      """
10      Returns the pool reward at a certain block height. The pool earns 7/8 of the reward in each block. If the farmer
11      is solo farming, they act as the pool, and therefore earn the entire block reward.
12      These halving events will not be hit at the exact times
13      (3 years, etc), due to fluctuations in difficulty. They will likely come early, if the network space and VDF
14      rates increase continuously.
15      """
16
17      if height == 0:
18          return uint64(int((7 / 8) * 300000 * _mojo_per_dogechia))
19      elif height < 3 * _blocks_per_year:
20          return uint64(int((7 / 8) * 2 * _mojo_per_dogechia))
21      elif height < 6 * _blocks_per_year:
22          return uint64(int((7 / 8) * 1 * _mojo_per_dogechia))
23      elif height < 9 * _blocks_per_year:
24          return uint64(int((7 / 8) * 0.5 * _mojo_per_dogechia))
25      elif height < 12 * _blocks_per_year:
26          return uint64(int((7 / 8) * 0.25 * _mojo_per_dogechia))
27      else:
28          return uint64(int((7 / 8) * 0.125 * _mojo_per_dogechia))
29
30
31  def calculate_base_farmer_reward(height: uint32) -> uint64:
32      """
33      Returns the base farmer reward at a certain block height.
34      The base fee reward is 1/8 of total block reward
35
36      Returns the coinbase reward at a certain block height. These halving events will not be hit at the exact times
37      (3 years, etc), due to fluctuations in difficulty. They will likely come early, if the network space and VDF
38      rates increase continuously.
39      """
40      if height == 0:
41          return uint64(int((1 / 8) * 300000 * _mojo_per_dogechia))
42      elif height < 3 * _blocks_per_year:
43          return uint64(int((1 / 8) * 2 * _mojo_per_dogechia))
44      elif height < 6 * _blocks_per_year:
45          return uint64(int((1 / 8) * 1 * _mojo_per_dogechia))
46      elif height < 9 * _blocks_per_year:
47          return uint64(int((1 / 8) * 0.5 * _mojo_per_dogechia))
48      elif height < 12 * _blocks_per_year:
49          return uint64(int((1 / 8) * 0.25 * _mojo_per_dogechia))
50      else:
51          return uint64(int((1 / 8) * 0.125 * _mojo_per_dogechia))
```

Figure 2: doge-chia/dogechia/consensus/block_rewards.py

Changes to **default_constants.py** include an adjustment to the following:

- `DIFFICULTY_CONSTANT_FACTOR` – DogeChia uses 2 ** 57 which differs from Chia which uses 2 ** 67. Thus the difficulty displayed in the DogeChia UI will be higher than Chia and Flax.
- `GENESIS_CHALLENGE` – DogeChia set this value to a different hash to ensure chain incompatibility with Chia and Flax.
- `GENESIS_PRE_FARM_POOL_PUZZLE_HASH` – DogeChia changed this value to a unique puzzle hash from both Chia and Flax ensuring the pool reward for the pre-farm is properly assigned.
- `GENESIS_PRE_FARM_FARMER_PUZZLE_HASH` – DogeChia changed this value to a unique puzzle hash from both Chia and Flax ensuring the farmer reward for the pre-farm is properly assigned.

Changes to **block_rewards.py** include an adjustment to the following:

- Lines 18 and 41 control the amount of pre-farm DogeChia created in the genesis block. This differs from Chia setting the amount to 300,000 and is unchanged from Flax. Though the amount is the same the puzzle hashes differ ensuring that the pre-farm is not assigned to the same address as the Flax pre-farm.

DogeChia also made changes to **dogechia/util/initial-config.yaml** namely the default ports used by the blockchain as well as indicating the domain for DNS introducer.

1.2 Co-Farming

Chia farming is notoriously boring for small farmers. Chia grew at an explosive and exponential rate to 30 XiB in early July of 2021.[7] This Netspace size means that using OG plots small Chia farmers (those with less than 1 PiB of plots) experience ETW in months or years and are faced with the choice of replotting to NFT and joining a pool or quitting altogether, potentially losing the investment on equipment and time.

With Chia forks becoming available, first with Chaingreen and Chiarose and later Flax, SPARE, Goji, and Seno farmers had an alternate path: co-farming smaller netspace coins with their existing Chia plots.

Chia had considered that other blockchains would adopt PoST consensus mechanisms and that Chia plots would be capable of re-use for co-farming.[8] It is no surprise that the first Chia forks arose shortly after Bram Cohen discussed the idea of co-farming. DogeChia was created at the beginning of the MOAR forks craze where over 30 new forks were created over the course of July and August 2021.

1.3 Experimentation and New Features

DogeChia differentiated itself beyond co-farming by demonstrating a willingness to integrate experimental code. With the 1.0.9 release of DogeChia, features buried in the Chia code were unearthed and made available to the broader public.[9] Coloured Coins, Rate Limited Wallets, and Distributed Identity Wallets were made available for programmers and DogeChia Full Node operators via the DogeChia Full Node UI. Though all of these features pre-exist in Chia from early testnet releases, no other fork made the UI available for use and ease of experimentation.[10]

DogeChia will use a next generation standard, based on the Chia CAT1 specification for issuance of special assets. This specification will be adapted for use on the DogeChia blockchain and will be referred to as *Digitial Operable Geld* (DOG) and will initially be available for use as the DOG1 standard.

DogeChia will establish a mechanism of reward for seeders of critical on-chain metadata and images. This will be a combination of an official blockchain oracle which incorporates information about seeders of torrent files associated with specific ecosystem metadata such as DOG icons and metadata and NFT image details for custom collectibles. Farmers will collect XDG or other DOG rewards associated with provably seeding critical data.

DogeChia will establish an ecosystem of collectibles through the issuance of images associated with mythology of the DogeChia origin and subsequent stories. Images associated with the illustrated origin story, wallet graphics, and images created by guest illustrators will be made available for auction. This will be done in a novel way where illustrators will have particular attribution (via Distributed Identity) and will receive a portion of the reward whenever the collectible is transferred.

The continued goal of DogeChia team is to pursue a fun ecosystem for creators and game programmers who utilize DogeChia and Chialisp programming to create fun experiences.

1.4 Marketing

DogeChia differentiated itself early in the MOAR forks phase through marketing campaigns in Discord, Twitter, Github, and Keybase. The efforts primarily focused on growing Netspace by targeting Chia fork farmers (those already co-farming Flax, Chaingreen, SPARE, Goji, and Seno) and disaffected Chia farmers not yet farming any forks.

These efforts saw DogeChia grow in Netspace from 100 PiB on 13/07/2021, to 200 PiB on 19/07/2021, to 300 PiB on 30/07/2021, to 400 PiB on 08/08/2021[11], to over 500 PiB by 31/08/2021[12]. This Netspace size represents 1.4% of the total Chia netspace at publication.

The next phase of marketing will target general users of blockchain technology as custodial exchanges and non-custodial light wallets enable users to acquire and hold DogeChia (XDG) without the need to run a full node. These efforts will commence in the winter of 2021 and continue as Chia is more widely adopted by mainstream exchanges while more forward looking exchanges start to experiment with Chia forks such as SPARE[13], HDD, Flax, Silicoin, FloraCoin, and DogeChia.

References

[1] All the Chia Forks, https://discord.gg/JVG68HfVyD

[2] Chia Fork Traders, https://discord.gg/ecqyVhMtVQ

[3] DogeChia GitHub, https://github.com/DogeChia/doge-chia/releases/tag/0.1.5

[4] Chia Greenpaper, https://www.chia.net/assets/ChiaGreenPaper.pdf

[5] DogeChia GitHub, https://github.com/DogeChia/doge-chia/blob/main/dogechia/consensus/default_constants.py

[6] DogeChia GitHub, https://github.com/DogeChia/doge-chia/blob/main/dogechia/consensus/block_rewards.py

[7] The Chia Plot - What is the real Chia netspace?, https://thechiaplot.net/2021/07/24/what-is-the-real-chia-netspace-we-may-have-an-answer/

[8] Youtube, https://www.youtube.com/watch?v=2uvlop-hlio&t=412s

[9] DogeChia GitHub, https://github.com/DogeChia/doge-chia/releases/tag/1.0.9

[10] The Chia Plot - Is Chia Fork DogeChia ahead of Chia on their own code?, https://thechiaplot.net/2021/07/26/is-chia-fork-dogechia-ahead-of-chia-on-their-own-code/

[11] Twitter, https://twitter.com/dogechia/status/1424535387310022657

[12] Twitter, https://twitter.com/dogechia/status/1432733404924194827

[13] Twitter, https://twitter.com/GetSpare/status/1435483099920429057