$TRAYACOIN

MAIN-NET UPGRADE TESTS

Motto: Leave no NAH behind

MAY 2018

Revision 1.1

Report by the Strayacoin Development Team

The Strayacoin development team involved in the testing are

- David (The KeyMaker) Higgins
- David Gilbert (Adelaide Creative)
- David Nicholls
- Allan Davis
- Aaron Lange-Bistrovic

Contents

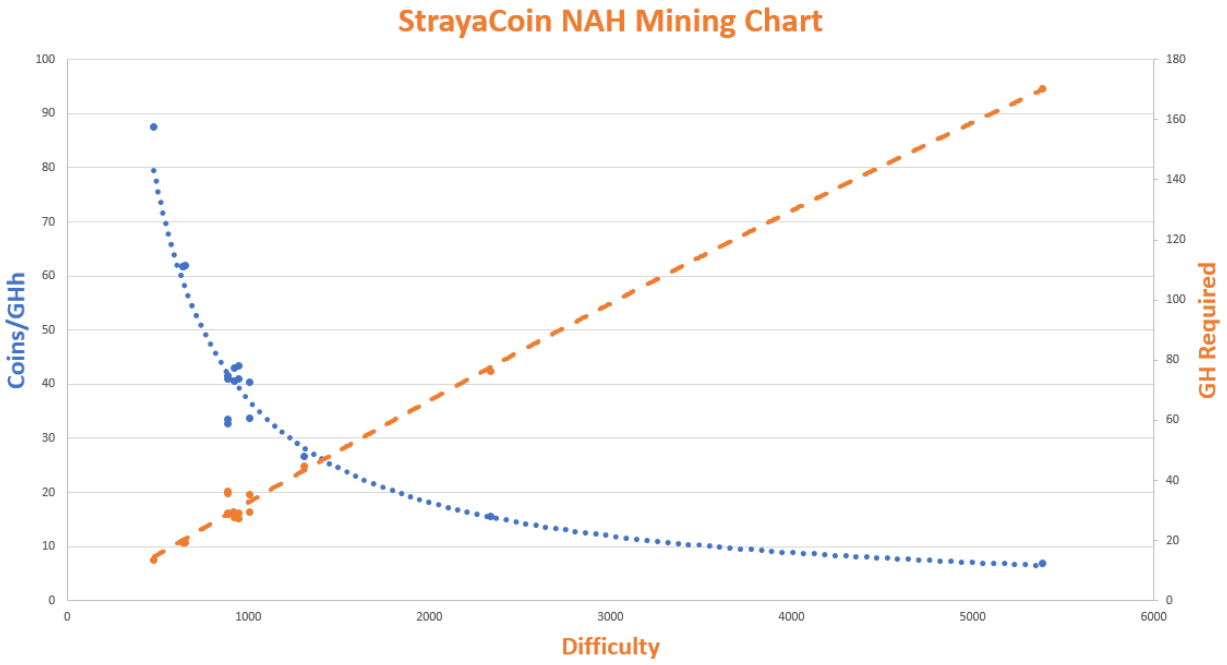
1. Introduction

Strayacoin was introduced on Australia Day, 2018 by Jack Hurley of Bendigo, Victoria, and had a great start, moving quickly with development and adoption.

It is a cryptocurrency, with maximum supply of 25 million, approximately 1/3 of Litecoin (84M), and slightly higher than Bitcoin (21M). As such, interest in the coin has been extremely high, both in the mining and transfer of coins on the exchanges.

Initial development of tools and wallets was quickly achieved, and also meant that there was ready access to mining pool software, which could be used by GPU's and ASIC's.

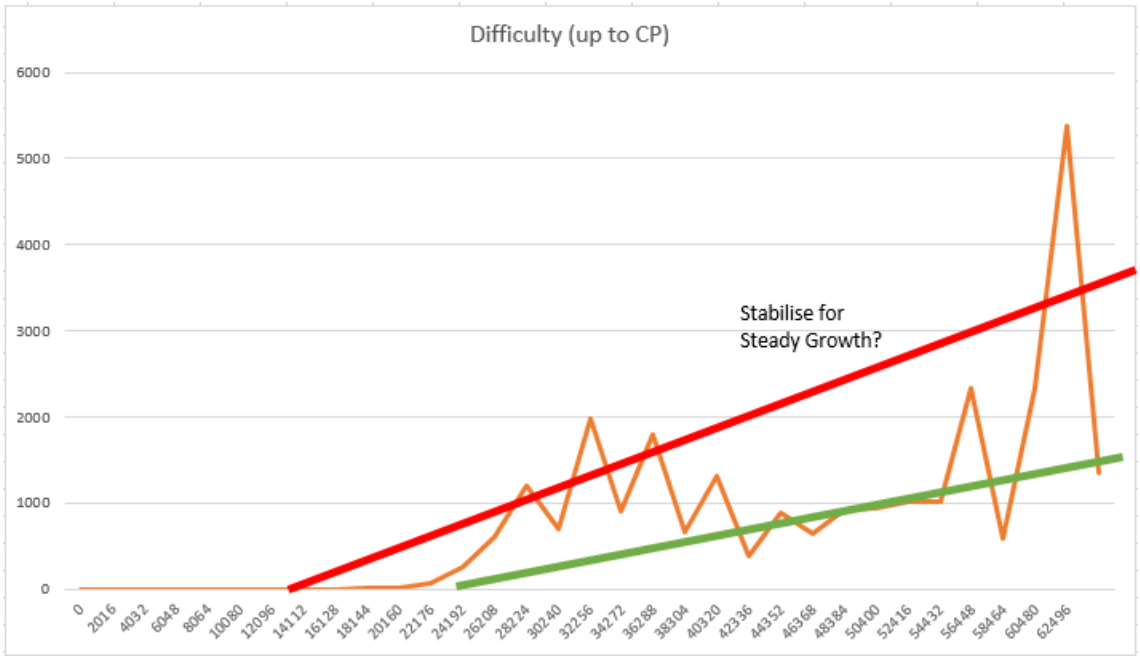
The transactions on the blockchain for the coin are secured using a Proof Of Work Hash function called "Scrypt", which is the same as Litecoin. Hash functions are calculated competitively between miners until one finds a "Nonce" to solve the maths problem for the current difficulty. The reward for solving the Nonce is the collection of the block reward, currently 50 coins. As the below chart shows, as the difficulty increases, the network Hashrate required increases, while the coins generated as the reward decrease on a per GH (giga-hash) basis.



The difficulty adjusts to the mining power every 2016 blocks, this is fine for Litecoin, which doesn't see a huge change in mining power directed at the blockchain for that coin over time.

For a young coin, and the availability of large rental Scrypt miners from sites such as MiningRigRentals.com and NiceHash.com, it is an issue, and avails the coin to low difficulty "coin hopping attack" whereby miners will buy hashpower only during times of low difficulty (cheaper per coin mining cost). During March, we started to see huge mining power directed at CageCoinPool, and the low difficulty exploited, and then the blockchain stagnating at high difficulty due to reluctance of miners to pay "far over the market price" of the coin to conduct mining.

As can be seen in the graph below, the current difficulty is above 5000, and next difficulty calculated at 1300 (minimum is set at ¼), and the cycle would be expected to repeat (4x increase again from 1300), unless there is significant appreciation in the coin price and stabilized miners.



The most efficient path is for the blockchain to consistently produce blocks every 2.5 minutes. Currently, this is not happening, with the current difficulty above 5000, blocks only being generated every 78 minutes currently (with 6GH network hashrate), and next difficulty change predicted 89 days from the last diff change, when it should be every 3.5 days.

	StrayaCoin Target Block Time	2.5	minutes
	StrayaCoin Target Block Time	3.50	days
	Current Difficulty	5386	
Next Checkpoint from now (estimated)		1794.6	hours
Next Checkpoint (Estimated) from last Checkpoint		89.2	days
	Next Checkpoint (Estimated)	7/08/2018 22:28	GMT
	Next Difficulty (estimated)	1347	

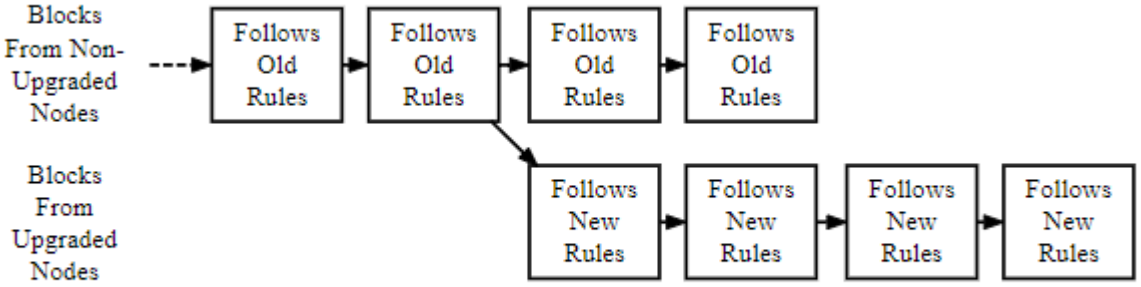
Thankfully, there are a number of ways this can be solved, so that the blockchain operates efficiently in future. Three options are available

a) Utilize a different Proof Of Work Algorithm which is ASIC resistant

b) Change the Difficulty Adjustment Interval to a lower value

c) Both of the above

All of these can be implemented on the existing blockchain using a process of updating the strayacoin-core QT software/integrated Windows Wallet. In this way, existing NAH holders are protected and taken forward with the changed rules. This is called a **hard fork,** shown below. For a fork to be considered successful, all nodes have to upgrade, and then no different new coins are made..ie..all developers and exchanges support the fork.



A Hard Fork: Non-Upgraded Nodes Reject The New Rules, Diverging The Chain

2. Exploring the options

Research was conducted on what other coins had done in similar situations. Web searches on coin forks, the reason why, and results were reviewed, and lively discussion ensued on the Strayacoin Discord channel.

Github provides a ready reference of code changes and when they were implemented on various coins. A number of coins moved to ASIC resistant algorithms or changed the difficulty adjustment.

2.1. Hash Algorithms

There are a myriad of different algorithms available. Some are listed below

- X11 (this means 11 different algorithms)
- Scrypt N – adaptive N factor
- Cryptonight

Alas, with popularity (coin price/incentive) comes innovation, and now all of these have ASIC's developed. It becomes an arms race with the cryptocurrency coins sometimes forking multiple times to try to stay ahead…so why do they want to stay ahead…because they don't want mining centralized, and they realize that for broad adoption and security, having distributed miners (using CPU or GPU's) is the best path.

This is a recent example from Monero on their fork to avoid asics.

https://cointelegraph.com/news/monero-hard-fork-appears-successful-as-devs-shun-bitmains-asic-miners

Currently, there are some great algorithms available, listing of some of them below

- Lyra2Re2
- X16R
- Allium

2.2. Difficulty Adjustment

A number of coins adapted the Difficulty Algorithm. Kimoto Gravity Well (KGW) was introduced, with an average of a small number of recent historical blocks used to adapt the difficulty on every block. The current "flavor of the month" is to use an adapted version of this called Dark Gravity Wave (DGW).

Below is an excellent article on diff adjustment

https://www.cryptocompare.com/coins/guides/what-is-a-kimoto-gravity-well-dark-gravity-wave-or-digishield/

2.3. Implications

With an existing chain, and many tool/wallet developments, it is critical to minimize the impact and carry forward as much as possible. In particular, the Android and IOS Wallets connect directly to the blockchain as SPV Clients (Secure Payment Verification). This means that they also validate the blocks presented to them, rejecting blocks and nodes that present invalid blocks (considered invalid by the rules embedded in their codebase). This must be considered so those platforms are upgraded at the same time if necessary.

3. Selected Tests

Moving forward with a consensus of path has been the most difficult task, with many opinions on which algorithm or difficulty adjustment is best. The following tests were identified as being easy to implement, while testing the necessary elements required.

3.1. Introducing SCRYPT-NAH (Non-ASIC-Hash)

Scrypt-NAH is a newly developed Hash function (by David Higgins and David Gilbert) based on Scrypt, so it has the same randomizing hash performance and close to the same speed of calculations/second. After the standard Scrypt hash function is calculated, the output is scrambled before passing to the Difficulty Check. This function will be ASIC and GPU resistant, especially if the scrambling method is not disclosed, requiring extensive reverse engineering to figure out what is going on.

It has been chosen because there are minimal changes to the existing codebase, which would be required not only in the strayacoin-qt, but also the Android and IOS wallets.

To test this algorithm, the Difficulty must be reset to the Genesis Difficulty, then the integrated CPU miner uses the hash function in the straya-core software iteratively to find the Nonce.

3.2. The Tests

The following three test scenarios have been decided on

1. Scrypt-NAH with diff reset to genesis diff
2. Scrypt-NAH / DGW - with diff reset to genesis diff
3. DGW - working down from existing diff, no reset

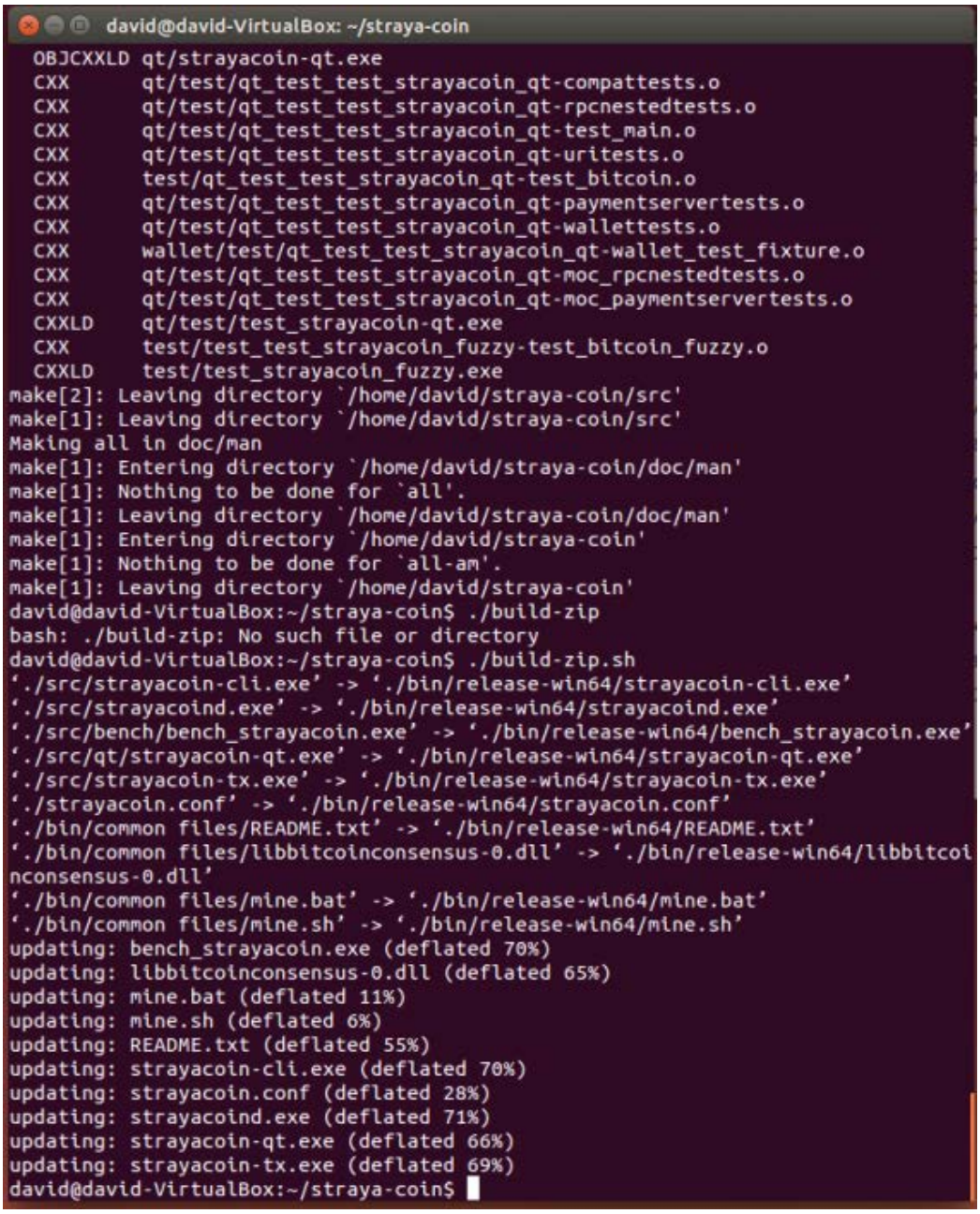
3.3. Implications

Forking an existing blockchain requires careful planning to ensure that any updates to the codebase are controlled in a test environment. Fortunately, live, on main-net testing can be conducted, because the blockchain actually protects itself from “attacks” with consensus of the rules being maintained among the peers, and banning of peers who don’t follow the rules.

The only requirement is that the updated strayacoin-qt software is limited in distribution so it doesn’t take over the majority of nodes through installs.

4. The Strayacon core software Tests

Strayacoin is developed in C++ (pronounced CPlusPlus), and cross compiled for Windows on Ubuntu Linux 14.04. Below shows that we are able to compile the existing code and build the distribution zip file.



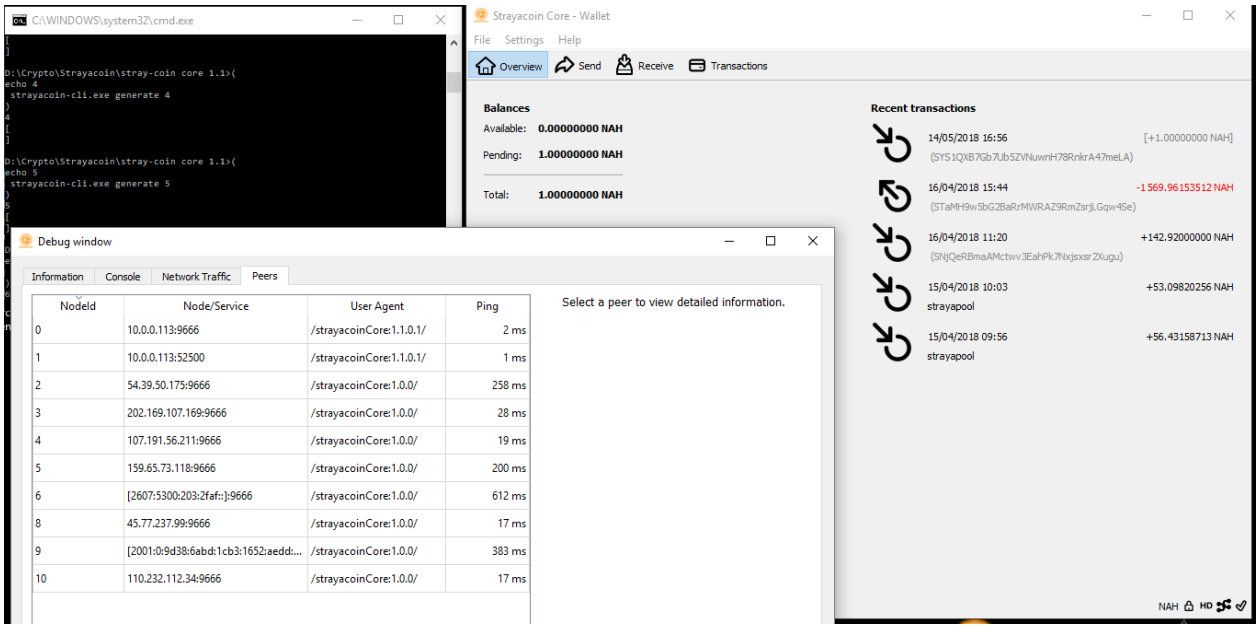
For each of the tests, the fork has to be arranged at a selected block height, with the old rules followed up to the selected block height, and new rules followed thereafter. One would expect existing nodes to reject blocks from the new nodes, and the new nodes rejecting the blocks from the existing nodes..hence a fork occurs.

From the approximately 100,000 lines of code in the Strayacoin core software, a total of 16 files have to be changed to allow for a fork at a selected block height

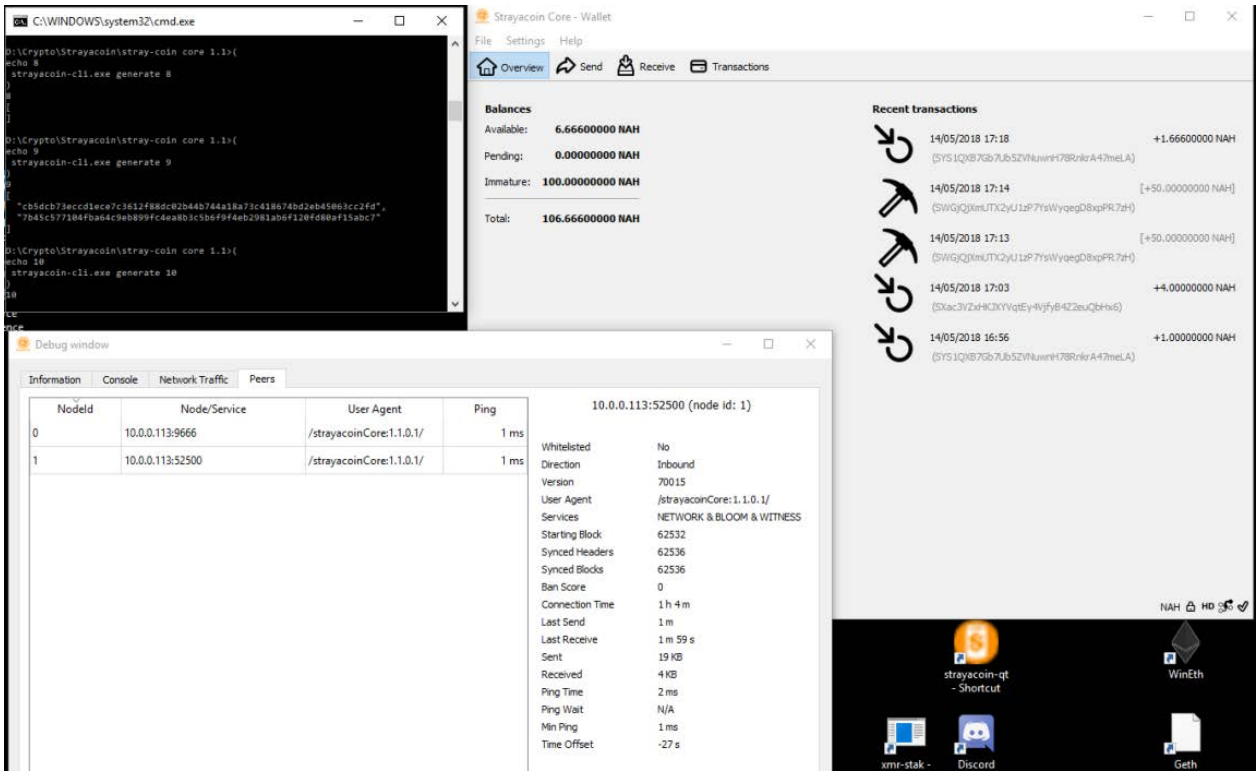
```
modified:   Makefile.am
modified:   configure.ac
modified:   src/Makefile.test.include
modified:   src/chain.h
modified:   src/chainparams.cpp
modified:   src/chainparams.h
modified:   src/crypto/scrypt.cpp
modified:   src/crypto/scrypt.h
modified:   src/primitives/block.cpp
modified:   src/primitives/block.h
modified:   src/rpc/mining.cpp
modified:   src/test/blockencodings_tests.cpp
modified:   src/test/crypto_tests.cpp
modified:   src/test/test_bitcoin.cpp
modified:   src/validation.cpp
modified:   src/validation.h
```

4.1. Scrypt NAH Test from Block 62533 (core version 1.1.0.1)

This test was begun on 14th May. The below picture shows two updated nodes connected to main-net, switching to Scrypt-NAH at next block, and miners set to mine when the next block ticks over. These two nodes should go forward with high block rate (lower diff)...but reject from all other nodes...



Below shows that other peers have dropped us...with successful mining on the updated node using the built in client. We tested the Android wallet..it cant sync past the fork..this is expected.



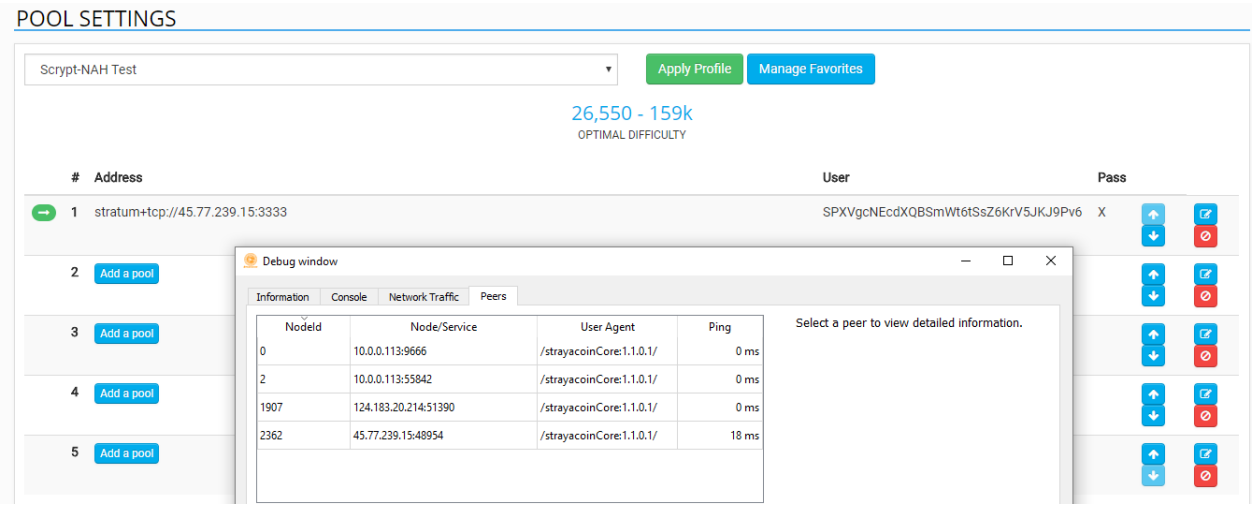
Successful test.

Further tests were conducted with 4 nodes among the development team, testing new and existing wallet synchronization. Tests successful.

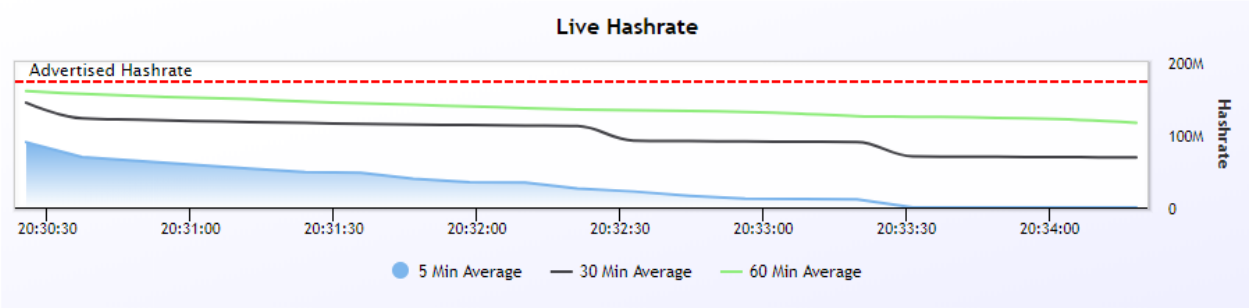
NodeId	Node/Service	User Agent	Ping
0	10.0.0.113:9666	/strayacoinCore:1.1.0.1/	0 ms
2	10.0.0.113:55842	/strayacoinCore:1.1.0.1/	0 ms
1907	124.183.20.214:51390	/strayacoinCore:1.1.0.1/	0 ms
2362	45.77.239.15:48954	/strayacoinCore:1.1.0.1/	20 ms

Next test – try to mine with Scrypt

A test mining pool was setup on 45.77.239.15. Below creen shows the MiningRigRentals pool configuration and nodes on our fork in the Strayacoin-QT software.



The following shows that the ASIC miner cannot mine on Scrypt-NAH.



What we were looking for is rejected blocks (not shares-they would be handled by the pool) because they don't meet the criteria. We use the Scrypt algo, but scramble the result with another algo prior to checking it against the proof of work target. So the 1.1.0.1 core full node checks when you submit a block to it..and then it will reject as not meeting the difficulty level.

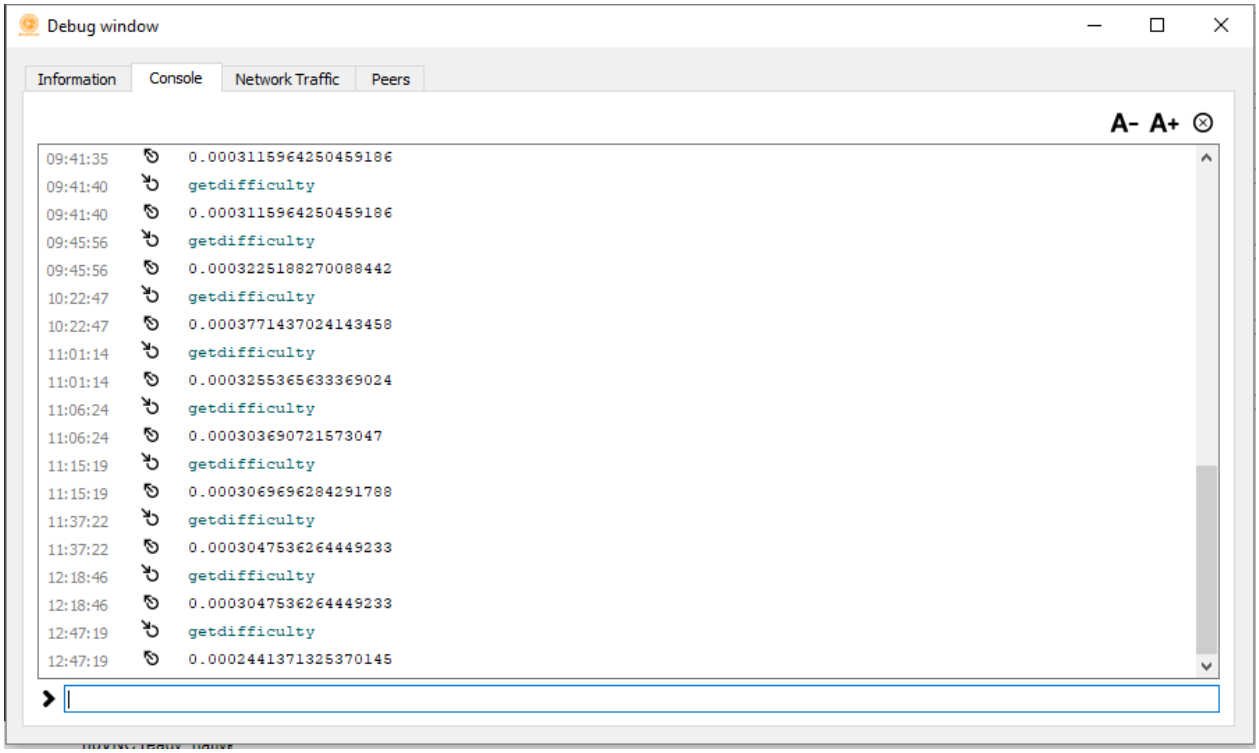
From this, it is evident that one cannot mine Scrypt-NAH with Scrypt ASIC miners. Success.

4.2. Scrypt NAH / DGW Test from Block 62670 (core version 1.1.0.2)

Dark Gravity Wave was added to the core software, and implemented from block height 62670 from the forked chain made during the above test. Once the block height was reached, the difficulty changed to the Genesis difficulty (0.0002..). A total of 4 CPU integrated miners were required before the difficulty started to rise.

```
08:59:40   0.0002441371325370145
09:30:24   getdifficulty
09:30:24   0.0002441371325370145
09:33:08   getdifficulty
09:33:08   0.0002561587545591451
09:41:35   getdifficulty
09:41:35   0.0003115964250459186
09:41:40   getdifficulty
09:41:40   0.0003115964250459186
```

Further tests were conducted by reducing the miners to 1, and watching the diff return to genesis diff.

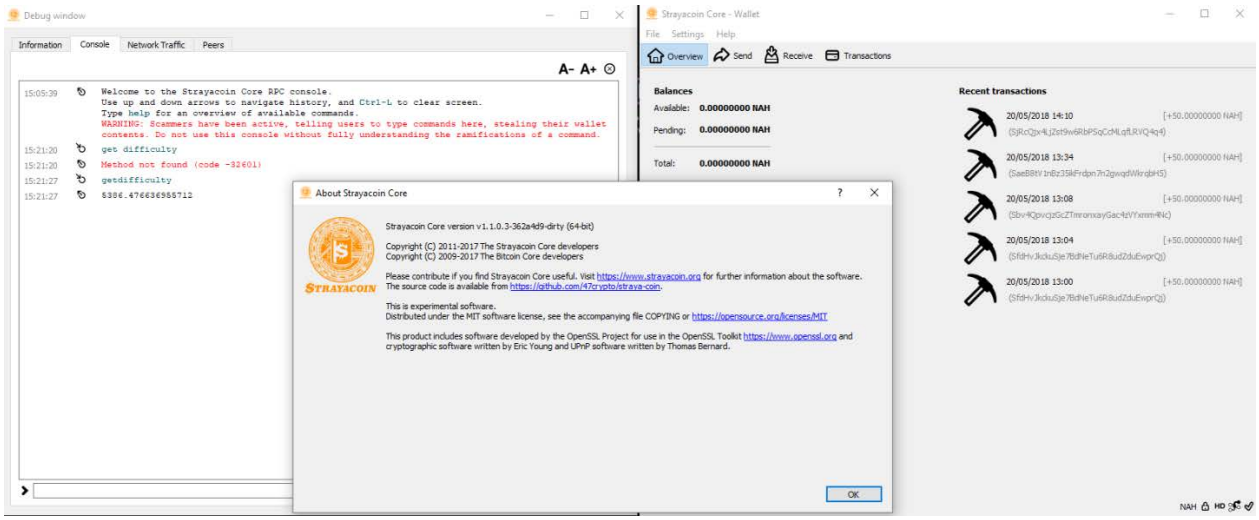


Success.

4.3. DGW Test from Block 62685 (core version 1.1.0.3)

Scrypt-NAH was removed, and the Dark Gravity Wave was added to the core software, and implemented from block height 62685. It was expected that the existing hash on the network would be accepted as the Difficulty dropped.

Below picture shows the core connected and re-synchronized to main-net. Also in the screenshot is the mining done when using scrypt-NAH..these transactions show in the history list, but not in the balance..they are "lost with the deleted fork"



After the selected block height , the updated nodes stopped accepting new blocks with below debug message...

“2018-05-20 08:53:46 ERROR: AcceptBlockHeader: Consensus::ContextualCheckBlockHeader: 77f028a6038b87408eb11cbcb85a79ee609392cb5d5cda6a1a2703249da25ab2, bad-diffbits, incorrect proof of work (code 16)”

We had thought it would accept the blocks from mainnet (since they were at a higher diff, (DGW would be lower)), but this hasn’t happened and getdifficulty or getmininginfo still shows the high diff, even though it showed up before when modified both scrypt-NAH and DGW and CPU mined locally. A little confused right now. Reviewing the code reveals…

validation.cpp, line 2924

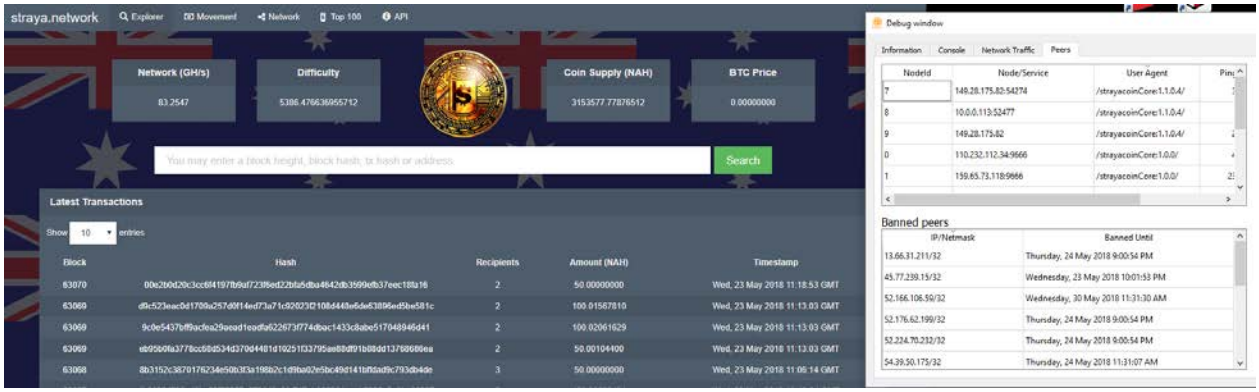
if (block.nBits != GetNextWorkRequired(pindexPrev, &block, consensusParams))

return state.DoS(100, false, REJECT_INVALID, "bad-diffbits", false, "incorrect proof of work");

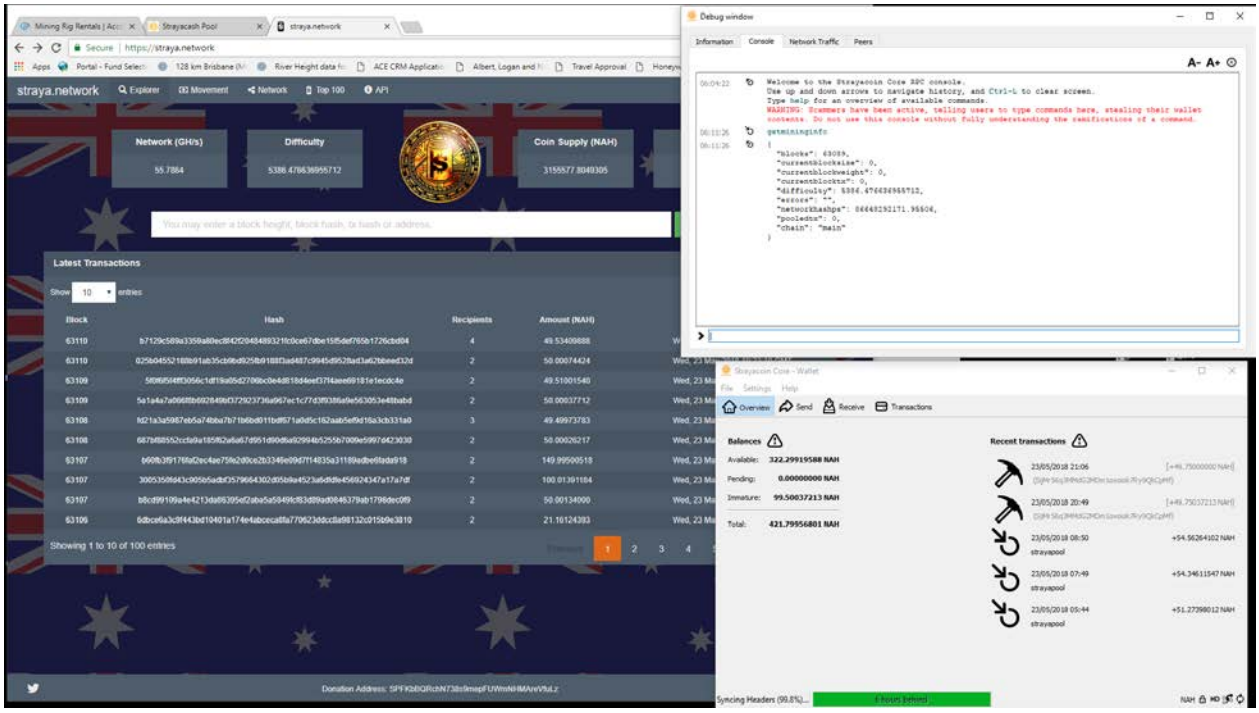
So..this means 1.1.0.3 core with DGW will not accept blocks submitted by nodes with incorrect hash..even if the proof of work done is greater than the DGW difficulty required

4.4. DGW Test from Block 63090 with Mining Pool (core version 1.1.0.4)

This test was begun on 23th May. Another mining pool was setup (thanks Davo - diabloblack.com). Then mining hash was directed at the pool. The updated nodes co-exist before the fork as shown below.

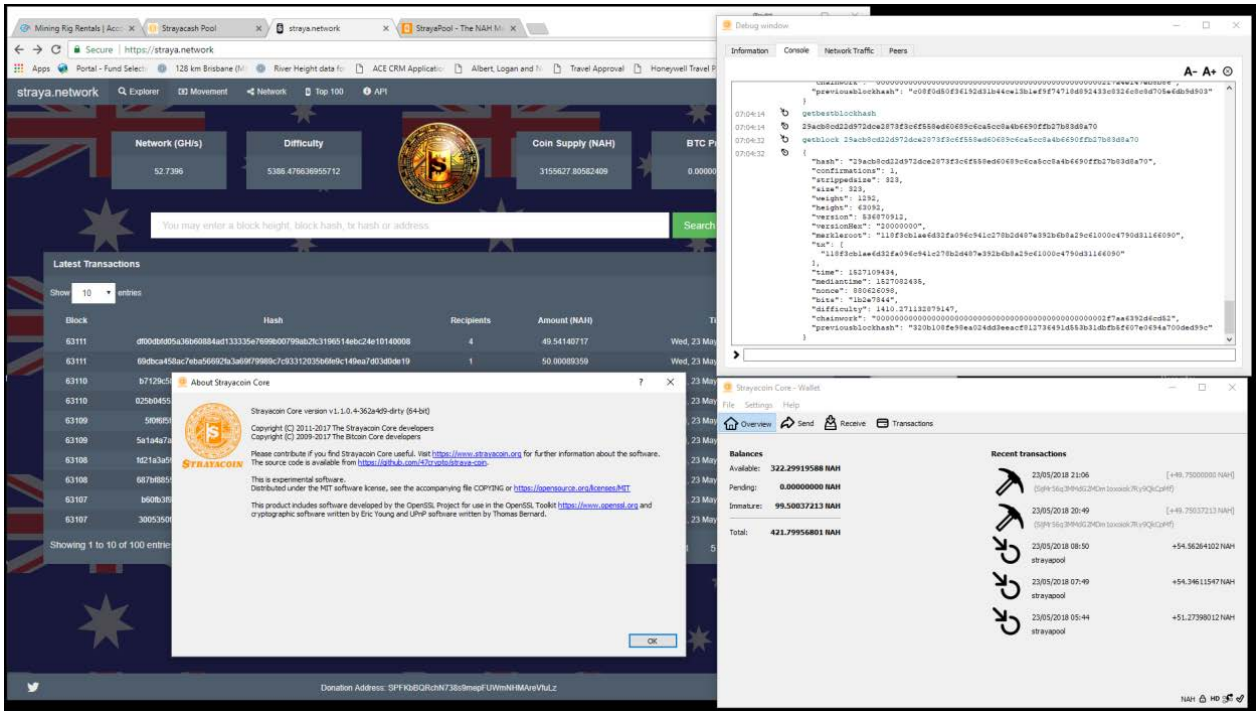


Below screenshot shows the forked nodes waiting to for an acceptable block at 63089.



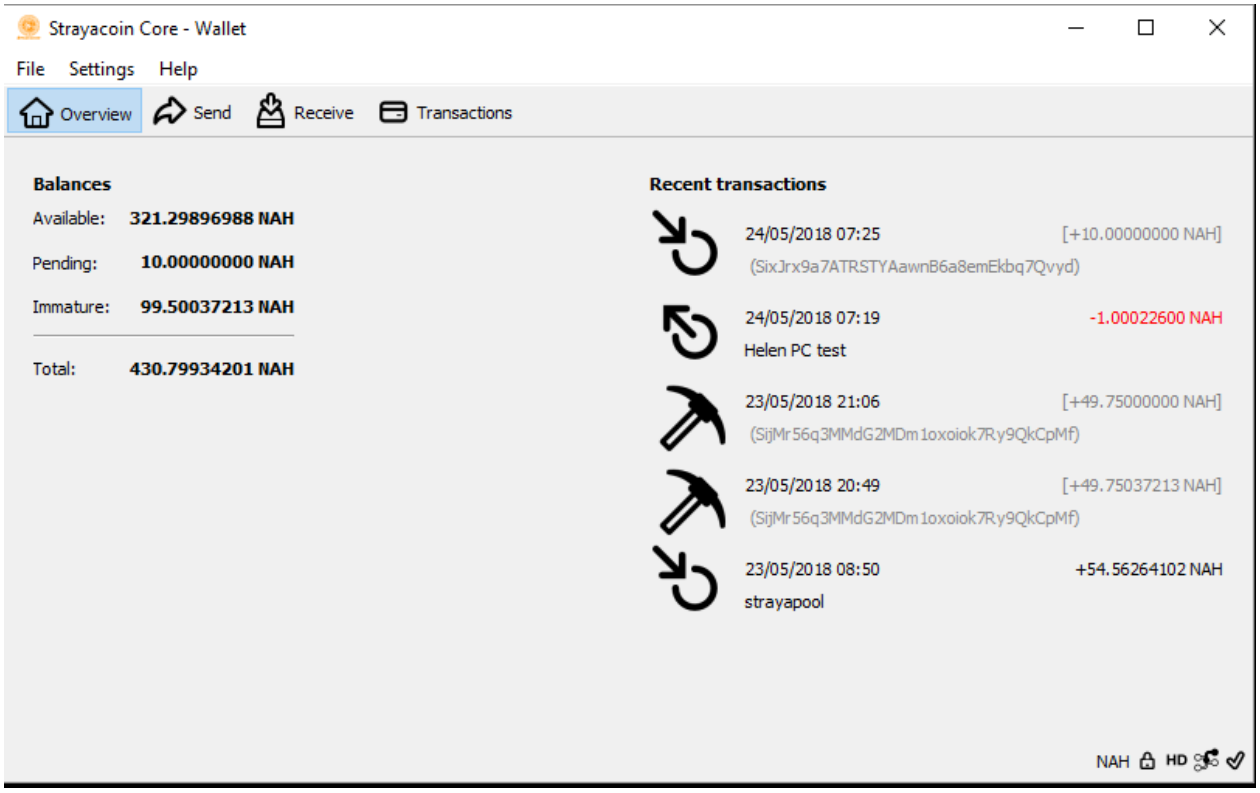
Below picture shows a successful fork, at block 63090, and diff drop !

In reference to the below screen capture, Block 63092 is shown on the right, after forking at 63090, it has a difficulty of 1410. I let it fork overnight..by morning...Mainnet continued on and is showing block 63111 in the straya.network webpage. It ran ahead, because the fork was waiting for a miner on a forked node (forked nodes only accept blocks with the exact required diff, rejecting mainnet blocks)... in the morning, a miner was put on a forked pool, and we had a hard test fork..it was stopped before overtaking mainnet, and the fork deleted. You can see the version of strayacoin core ..1.1.0.4.



After the fork, the android wallet was synchronized to one of the forked nodes, and 10NAH was sent from the android wallet to the Windows Wallet.

The below screenshot shows a successful send of 10NAH. It works without modification to android (or IOS) source-code!



5. Conclusion

After more than a month of investigation and testing, Strayacoin is ready for the future, and can change the algo or difficulty adjustment, or both.

The development team is expanding in experience, and it will be possible to make the changes on the existing blockchain, carrying all NAH holders with us.

Thanks for reading all the way to the end…this is just the beginning.