X16S

Sixteen shuffled algorithms
Designed for small miners

Luke Pighetti
March 22, 2018

Background

The X16R (random) algorithm was launched on the Ravencoin network in late 2018. This new algorithm provided an innovative method of ASIC resistance.

X16R used algorithms from X15, added SHA512, and then randomized the order by referencing the last sixteen digits of the previous block hash.

```
0  blake      6  luffa       c  fugue
1  bmw        7  cubehash    d  shabal
2  groestl    8  shavite     e  whirlpool
3  jh         9  simd        f  sha512
4  keccak     a  echo
5  skein      b  hamsi
```

Given the last sixteen digits of the previous block hash

```
4f0da52072c99492
```

X16R would complete a single hash cycle in the order below

```
4 keccak, f sha512, 0 blake, d shabal, a echo,
   5 skein, 2 groestl, 0 blake, 7 cubehash,
2 groestl, c fugue, 9 simd, 9 simd, 4 keccak,
             9 simd, 2 groestle
```

We notice that `groestl` and `simd` both repeat three times, weighting the hashrate and power consumption during this block 37% towards the characteristics of these two algorithms.

In practice, a GPU miner on the X16R algorithm that normally demands 600W will fluctuate between ~450W and ~800W, changing every block. The hashrate will similarly fluctuate, making it difficult to tune a mining rig for efficiency or productivity.

These power spikes reduce power-supply efficiency and lifespan. Our new algorithm, X16S, aims to solve these problems.

Introducing X16S (shuffle)

The X16S (shuffle) algorithm uses the last sixteen digits of the previous block hash to reorder a list containing all sixteen algorithms. It employs the same individual algorithms found in X16R.

```
0  blake      6  luffa      c  fugue
1  bmw        7  cubehash   d  shabal
2  groestl    8  shavite    e  whirlpool
3  jh         9  simd       f  sha512
4  keccak     a  echo
5  skein      b  hamsi
```

Given the last sixteen digits of the previous block hash

```
4f0da52072c99492
```

X16S would first reorder a list by the value of each digit found within the last sixteen digits of the previous block hash to reference an index within a list containing all algorithms.

```
   0123456789abcdef
4  4012356789abcdef
f  f4012356789abcde
0  f4012356789abcde
       . . .
9  0325a1c8f4679bde
2  2035a1c8f4679bde
```

The final order would then be

```
2035a1c8f4679bde
```

We then notice that the algorithms are never repeated or omitted, yet they are still randomly selected using the last sixteen digits from the previous block hash. This provides all the benefits of X16R while vastly improving the hashrate and power consistency. This makes it much better for small miners, further promoting decentralization.