Lyra2RE – A new PoW algorithm for an ASIC-free future

-- The Vertcoin Developers

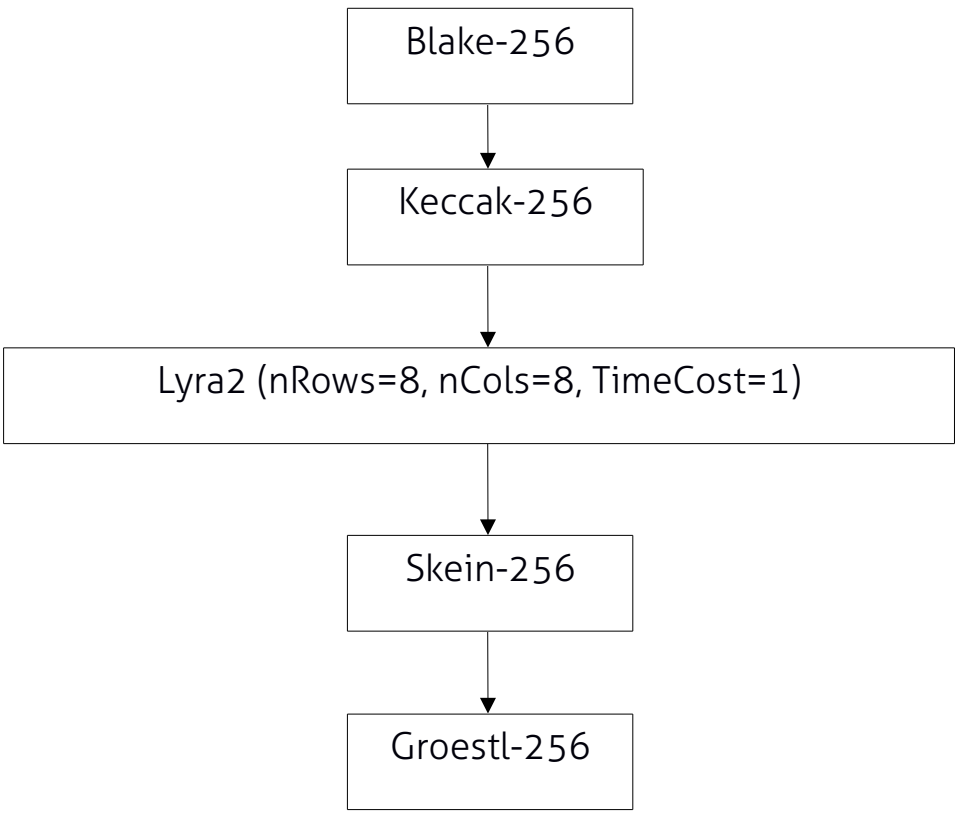
Abstract

We present "Lyra2RE" (RE – Reduced Efficiency), a NIST5 based chained algorithm with customizable parameters useful for thwarting future ASIC (Application Specific Integrated Circuit) threats. Vertcoin set out back in January 2014 with the express purpose of decentralization and ASIC resistance and almost a year on the dream is still alive.

However, in order to continue that dream we have to make changes when challenges arise and thus Lyra2RE will replace Scrypt-N as Vertcoin's PoW algorithm due to the existence of Scrypt-N ASICs. Another challenge we set out to overcome was the reduction of Vertcoin's mining power consumption; Lyra2RE is specifically designed with this purpose in mind affording lower power consumption and cooler GPU temperatures. Unlike Scrypt, Lyra2 (the principal part of the chained algorithm) allows us to change memory usage and time cost independently, giving us more leverage against ASICs.

Algorithm Design

Lyra2RE is a chained algorithm consisting of five different hash functions: Keccak, Skein, Groestl, Blake and Lyra2.



Leveraging industry proven hashing algorithms, we were able to create the most secure, robust, enduring chained algorithm to date that is both easier on GPUs and resistant to ASICs. At this time we have decided not to implement an "N factor" schedule as it is nearly impossible to predict the future. However, Lyra2RE will give us the flexibility to make changes whenever that becomes necessary.

Due to the chained nature of the algorithm, GPU miners will be inherently hard to optimize, meaning that power draw and heat can be reduced. This has been a desired feature for some time with Scrypt-N coins seeing dropping hashrates due to high energy consumption, despite Vertcoin having consistently the highest $/Day/Normalized MH/s than other coins [1].

As was previously detailed in the Lyra2 white paper [2], Lyra2 is strictly sequential in nature, using a "cryptographic sponge" at its core. This means that parallelization of the algorithm will be practically impossible with each step relying on the previous step having already been computed.

Unlike Scrypt-N, time cost and memory cost are separated, giving us independent control over both parameters. ASICs have been far easier to develop for Scrypt-N than they will be for Lyra2RE because increasing

the N-factor of Scrypt simply involves doing more iterations of the algorithm. Under Lyra2, whilst increasing the time cost only involves more iteration, increasing the memory requirement means that any potential ASIC device would have to physically be designed with more memory for each thread. In the future, if ASICs ever were developed for Lyra2RE, we would simply have to fork to a higher memory requirement and those ASICs would no longer properly function.

Summary

Many crypto-currencies claim to have ASIC-resistant algorithms, but many of them are only so because no ASIC has been made for them yet. It has been rumored that FPGAs for X11 already exist [3] and Neoscrypt only uses more rounds of cipher functions [4]. By contrast, Lyra2RE aims to be ASIC-resistant at heart, allowing for less disruption to miners in the future due to our ability to change algorithm parameters rather than change algorithm all together. It will also free up development time to focus on new features without having to worry about constantly implementing new algorithms every time there is an ASIC threat.

References

1. http://www.coinwarz.com/cryptocurrency/?scrypthr=450.00&scryptp=0.00&scryptc=true&scryptnhr=235.00&scryptnp=0.00&scryptnc=true&x11hr=1900.00&x11p=0.00&x11c=true&x13c=false&keccakc=false&quarkc=false&groestlc=false&jhac=false&blake256c=false&neoscryptc=false&e=Cryptsy&sort=avgprofit&dir=desc
2. http://lyra-kdf.net/Lyra2ReferenceGuide.pdf
3. https://bitcointalk.org/index.php?topic=586407.0
4. http://www.feathercoin.com/neo-scrypt-press-release.pdf