X16R

ASIC Resistant by Design

Tron Black and Joel Weight

The history of hashing for cryptocurrencies began with SHA256 for Bitcoin, then Scrypt for Litecoin, Equihash for Ethereum, X11 for Dash, followed by X13, X15, and X17. X16R is the next step in this evolution to find a better mining algorithm.

The reason for the algorithm changes is to minimize the impact of purpose-built hardware on the mining ecosystem of the coin. Bitcoin was originally intended to be mined by computers everywhere. As the value of bitcoin increased, it became advantageous to mine in parallel on hardware designed for parallel processing, so the mining moved to Graphics Processing Units (GPUs). As the economic value of mining further increased, it became economically viable to use programmable hardware in the form of Field-programmable Gate Arrays (FPGAs), which had an advantage over CPUs and GPUs. The next step was to build custom chips that are purpose-built for mining. These Application Specific Integrated Circuits (ASICs) were able to dominate the competing technologies and made it impractical to mine any other way. The last, and likely final, iteration for Bitcoin mining is the move to faster and more energy efficient ASIC hardware.

The unfortunate side-effect of this transition to ASIC hardware is the centralization of mining. While anyone can order these ASICs, there is an advantage to being near the manufacturing facility as shipping time is reduced. Additionally, access to cheap electricity is a priority, as the electricity used is the variable cost of the mining operation. This has led to some centralization of mining in China because of the proximity to ASIC development and the availability of inexpensive electricity in some provinces.

One solution to minimize the impact of ASIC miners is to use a memory intensive hashing algorithm. This is the approach of Scrypt, used by Litecoin, and Equihash, used by Ethereum. These two algorithms have reduced the impact of ASICs. While there are some ASIC miners for Scrypt, the relative advantage over GPUs is negligible. There are currently no ASIC miners for Equihash.

Another approach is to use a sequence of hashing algorithms where the output of one becomes the input to the next. Dash, formerly DarkCoin, took this approach with their X11 algorithm. X11 uses eleven chained hashing algorithms[1] in an effort to thwart the move to ASIC mining.

This approach worked for a while, but several manufacturers now produce ASIC miners for X11. The concept behind X11 can be extended to additional algorithms. For this reason, some coins use X13, some X15, and even X17 which chains seventeen hashing algorithms.

---

[1] https://getpimp.org/what-are-all-these-x11-x13-x15-algorithms-made-of/

The fixed order of hashing algorithms lends itself to the construction of ASICs. While chaining more algorithms together adds difficulty in constructing an ASIC, the X13, X15, and X17 all use the same ordering of hashing algorithms as the X11. This is likely to lead to faster manufacturing of ASICs for these algorithms as manufacturers only need to extend their existing design to accommodate the additional hashing algorithms.

The X16R algorithm intends to solve this problem by constantly disrupting the ordering of the hashing algorithms. The hashing algorithms are the same proven algorithms used in X15 + SHA512, but the ordering is changed based on the hash of the previous block.

This reordering does not make an ASIC impossible to build, but it does require that the ASIC adapts to additional input, which is more easily accomplished by a CPU or GPU. The reordering also prevents a simple extension of the current X11 ASICs or future X15 ASICs.

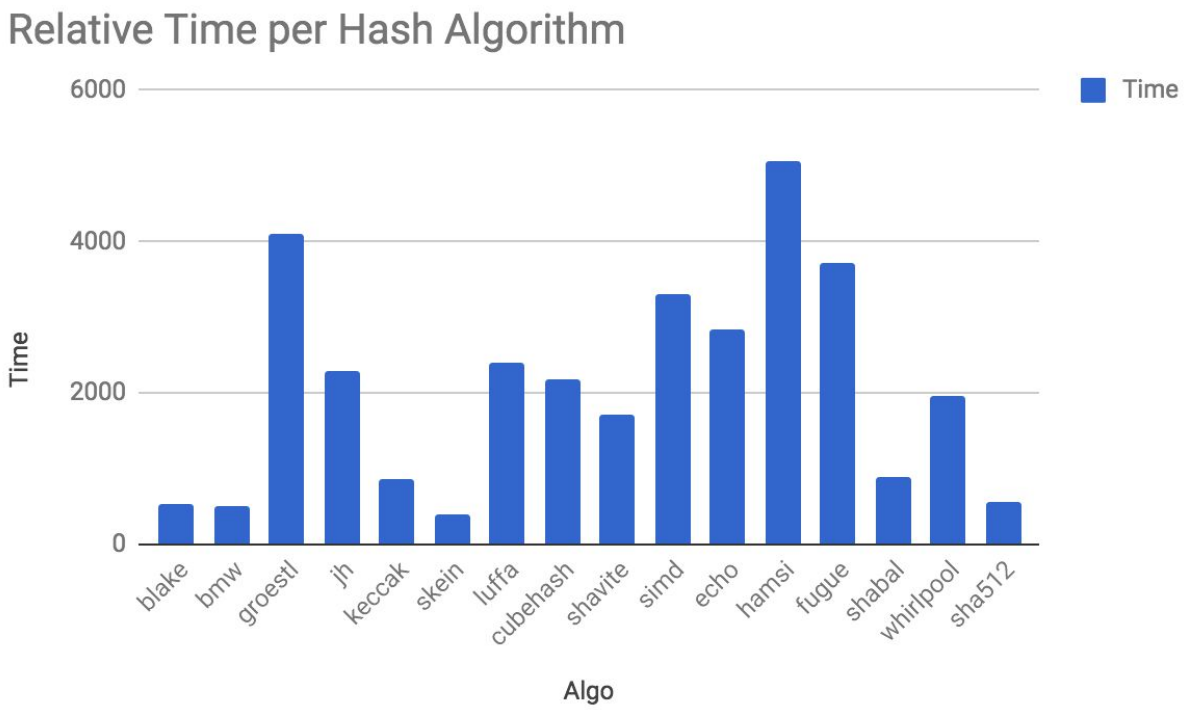
The X16R hashing algorithm consists of 16 hashing algorithms operating in chain fashion with the ordering dependent on the last 8 bytes (16 nibbles) of the hash of the previous block. The algorithms are as follows:

0=blake
1=bmw
2=groestl
3=jh
4=keccak
5=skein
6=luffa
7=cubehash
8=shavite
9=simd
A=echo
B=hamsi
C=fugue
D=shabal
E=whirlpool
F=sha512

Example:
Previous Block Hash:
00000000000000000007e8a29f052ac2870045ae3970270f9***7da00919b8e86287***

The final 8 bytes: **0x7da00919b8e86287**

Each hex digit (nibble) determines which algorithm to use next.
cubehash -> shabal -> echo -> blake -> blake -> simd -> bmw -> simd -> hamsi -> shavite -> whirlpool -> shavite -> luffa -> groestl -> shavite -> cubehash



Some of the hash algorithms take longer than others. This time differential tends to average out across the 16 algorithms while mining each block.

The test platform for this mining algorithm is Raven (RVN). Raven was launched on January 3, 2017, the 9th year anniversary of Bitcoin's launch. Raven changes the issuance schedule, block time, and mining algorithm.

Raven is the reference implementation for X16R, which defines the number of algorithms, the specific hashing algorithms used, the order of the algorithms, and the order of and bytes used from the previous block hash.

The concepts behind X16R could be extended to include Scrypt, Equihash, and other ASIC resistant algorithms to continue to allow anyone with an idle computer to participate in mining with off-the-shelf hardware. The ordering of the algorithms can easily be changed for each coin in order to dissuade hardware manufacturers from building ASICs for an entire class of coins as with X11.