|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Thông số** | **Bitcoin** | **Litecoin** | **Ethreum** | **Monero (XMR)** | **Dash (DASH)** |
| **Giới hạn coin** | 21 triệu | 84 triệu | Unlimited | Unlimite | Unlimite |
| **Thuật toán** | **SHA-256** | **Scrypt** | **Ethash**  **Keccak256** | **CryptoNight**  **CryptoNote** | **X11** |
| **Đơn vị tính hash** | G hash/s = triệu hash/s | K hash/s | M hash/s | Hash/s | M hash/s |
| **Thời gian tạo khối trung bình** | 10 phút | 2.5 phút | 13-15s | 60 s | 2 – 5 phút |
| **Thiết bị** | GPU, ASIC | GPU, CPU, ASIC | GPU  (ASIC resistance) | GPU, CPU | GPU |
| **Đặt lại độ khó** | 2016 khối | 2016 khối |  |  |  |
| **Tác giả** | Satoshi Nakamoto | Charles Lee | **Vitalik Buterin.** | Wladimir J. Van der Laan | Evan Dufield |
| **Ngày tạo ra** | 3/01/2009 | 7/10/2011 | 30/06/2015 | 18/04/2014 | 3/2015 |

Cryptocurrency Mining Hash Algorithms

[September 23, 2017](http://www.bitcoinlion.com/cryptocurrency-mining-hash-algorithms/) [nadavtal01](http://www.bitcoinlion.com/author/nadavtal01/) [2 Comments](http://www.bitcoinlion.com/cryptocurrency-mining-hash-algorithms/" \l "comments)

Different Types Of Cryptocurrency Algorithms

First, we need to understand what is it “Hash”?  
Hash is a “message digest” – a number generated from a string of text, the hash itself is smaller than the text, it is almost not possible to generate another string of text with the same hash value. Learn more about [hashes](https://en.wikipedia.org/wiki/Hash_function) – Wikipedia

Second, we need to understand what is it “Hashing Algorithm”  
Hashing algorithm is a Cryptographic hash function, mathematical algorithm that maps data of arbitrary size to a hash of a fixed size. Hashing algorithm being used for digital signatures and authentication.

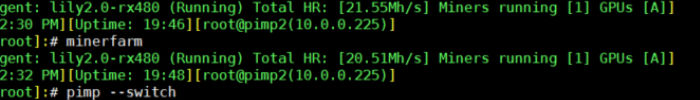
The Most Common Cryptocurrency Mining Algorithms

SHA-256 Algorithm:

SHA stand for “Secure hash Algorithm” (SHA-256) generates unique 256-bit (32-byte) signature for a text string. Block processing time for SHA-256 generally ranges from six to ten minutes and requires hash rates at the Giga hashes per second (GH/s). SHA-256 hash rate is measured by **GH/s:** Gigahashes per second, or one billion hash computations per second. SHA-256 algorithm mining can be performed on an [ASIC hardware](https://en.bitcoin.it/wiki/ASIC)(application-specific integrated circuit)  
**The SHA -256 cryptocurrency algorithm is used to mine:**

BitcoinCash (BCH)  
Bitcoin (BTC)  
21Coin (21)  
Peercoin (PPC)  
Namecoin (NMC)  
Unobtanium (UNO)  
Betacoin (BET)  
Bytecoin (BTE)  
Joulecoin (XJO)  
Devcoin (DVC)  
Ixcoin (IXC)  
Terracoin (TRC)  
Battlecoin (BCX)  
Takeicoin (TAK)  
PetroDollar (P$)  
Benjamins (BEN)  
Globe (GLB)  
Unicoin (UNIC)  
Snowcoin (SNC)  
Zetacoin (ZET)  
Titcoin (TIT)

Scrypt Algorithm:



Scrypt algorithm requires large amounts of memory and there was a need design it to perform large-scale custom hardware attacks. The Scrypt algorithm is more simple and quicker than the SHA-256 algorithm.  
Scrypt’s hash rate is measured by **KH/s:** Kilohashes per second, or one thousand hash computations per second.

Scrypt algorithm mining can be performed on a computer CPU, Graphics Processing Unit (GPU), there are some ASICs hardware that are available for Scrypt mining.  
**The Scrypt cryptocurrency algorithm is used to mine:**

Litecoin (LTC)  
Dogecoin (DOGE)  
Novacoin (NVC)  
WorldCoin (WDC)  
Latium (LAT)  
FeatherCoin (FRC)  
Bitmark (BTM)  
TagCoin (TAG)  
Ekrona (KRN)  
MidasCoin (MID)  
DigitalCoin (DGC)  
Elacoin (ELC)  
Anoncoin (ANC)  
PandaCoins (PND)  
GoldCoin (GLD)

X11 Algorithm:

The X11 hashing algorithm created by Dash core developer Evan Duffield. The X11 use a sequence of eleven scientific hashing algorithms for the proof-of-work. One of the bigest benefit of using X11 algorithm is the energy efficiency, GPUs require approximately 30% less wattage and run 30-50% cooler than they do with Scrypt.  
X11’s hash rate is measured by**MH/s:** Megahashes per second, or one million hash computations per second.  
**The X11 cryptocurrency algorithm is used to mine:**

Dash (DASH)  
CannabisCoin (CANN)  
StartCoin (START)  
MonetaryUnit (MUE)  
Karmacoin (Karma)  
XCurrency (XC)

Cryptonight Algorithm:

The Cryptonight algorithm was designed to be suitable for PC CPUs, it was implemented in an open sourced protocol which allows to increase privacy in cryptocurrency transactions – “CryptoNote”.  
Unlike the Scrypt algorithm the Cryptonight algorithm depends on all the previous blocks for each new block.  
Cryptonight’s hash rate is measured by**H/s:** Hashes per second, hash computations per second.  
**The Cryptonight cryptocurrency algorithm is used to mine:**

Monero (XMR)  
Bytecoin (BCN)  
Boolberry (BBR)  
Dashcoin (DSH)  
DigitalNote (XDN)  
DarkNetCoin (DNC)  
FantomCoin (FCN)  
Pebblecoin (XPB)  
Quazarcoin (QCN)

Dagger Hashimoto – Ethash Algorithm:

**Dagger Hashimoto** is a proposed spec for the mining algorithm for Ethereum and builds on two key pieces of previous work:

1. **Dagger:** algorithm by [Vitalik Buterin](https://en.wikipedia.org/wiki/Vitalik_Buterin), Dagger was meant to be an alternative to existing memory-hard algorithms like Scrypt, which are memory-hard but are also very hard to verify when their memory-hardness is increased to genuinely secure levels. However, Dagger was proven to be vulnerable to shared memory hardware acceleration by Sergio Lerner and was then dropped in favor of other avenues of research.

2. **Hashimoto:** algorithm by Thaddeus Dryja which intends to achieve ASIC resistance by being IO-bound, ie. making memory reads the limiting factor in the mining process. Hashimoto uses the blockchain as a source of data, simultaneously satisfying.

(source: “[Etherum / WIKI](https://github.com/ethereum/wiki/blob/master/Dagger-Hashimoto.md)“)

**Dagger Hashimoto’s**hash rate is measured by**MH/s:** Megahashes per second, or one million hash computations per second.  
**The Dagger Hashimoto – Ethash algorithm is used to mine:**

Ethereum (ETH)  
Ethereum Classic (ETC)  
Expanse (EXP)