WHAT IS THE DIFFERENCE BETWEEN LITECOIN AND BITCOIN?

WHAT IS THE DIFFERENCE BETWEEN LITECOIN AND BITCOIN?

In 2009, Satoshi Nakamoto launched bitcoin as the world's first cryptocurrency. The code is open source, which means it can be modified by anyone and freely used for other projects. Many cryptocurrencies have launched with modified versions of this code, with varying levels of success.

LITECOIN

Litecoin was announced in 2011 with the goal of being the 'silver' to bitcoin's 'gold'. At the time of writing, Litecoin has the highest market cap of any mined cryptocurrency, after bitcoin.

DIFFERENCE BETWEEN BITCOIN AND LITECOIN.

	BITCOIN	LITCOIN
COIN COUNT	21 MILLON	84 MILLION
ALGORITHM	SHA-256	SCRYPT
MEAN BLOCK TIME	10 MINUTES	2.5 MINUTES
DIFFICULTY TARGET	2016 BLOCK	2016 BLOCK
BLOCK REWARD DETAILS	HALVED EVERY 210,000 BLOCKS	HALVED EVERY 840,000 BLOCKS
INITIAL REWARD	50 BTC	50 LTC
CURRENT BLOCK REWARD	25 BTC	50 LTC
CREATED BY	SATOSHI NAKAMOTO	CHARLES LEE
CREATION DATE	JANUARY 3RD, 2009	OCTOBER 7th, 2011
MARKET CAP	$10,467,596,650.78	$540,274,528.26

MorCryp

BITCOIN STATISTICS VS LITECOIN STATISTICS

MINING DIFFERENCES

Just like bitcoin, litecoin is a crytocurrency that is generated by mining. Litecoin was created in October 2011 by former Google engineer Charles Lee. The motivation behind its creation was to improve upon bitcoin. The key difference for end-users being the 2.5 minute time to generate a block, as opposed to bitcoin's 10 minutes. Charles Lee now works for Coinbase, one of the most popular online bitcoin wallets.

ASIC Mining

ASIC Mining

For miners and enthusiasts though, litecoin holds a much more important difference to bitcoin, and that is its different proof of work algorithm. Bitcoin uses the SHA-256 hashing algorithm, which involves calculations that can be greatly accelerated in parallel processing. It is this characteristic that has given rise to the intense race in ASIC technology, and has caused an exponential increase in bitcoin's difficulty level.

Litecoin, however, uses the scrypt algorithm – originally named as s-crypt, but pronounced as 'script'. This algorithm incorporates the SHA-256 algorithm, but its calculations are much more serialised than those of SHA-256 in bitcoin. Scrypt favours large amounts of high-speed RAM, rather than raw processing power alone. As a result, scrypt is known as a 'memory hard problem'.

The consequences of using scrypt mean that there has not been as much of an 'arms race' in litecoin (and other scrypt currencies), because there is (so far) no ASIC technology available for this algorithm. However, this is soon to change, thanks to companies like Alpha Technologies, which is now taking preorders.

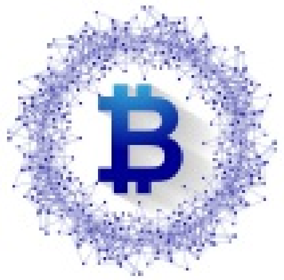
BITCOIN MINING RIG

GPU Mining

To highlight the difference in hashing power, at the time of writing, the total hashing rate of the bitcoin network is over 20,000 Terra Hashes per second, while litecoin is just 95,642 Mega Hashes per second.

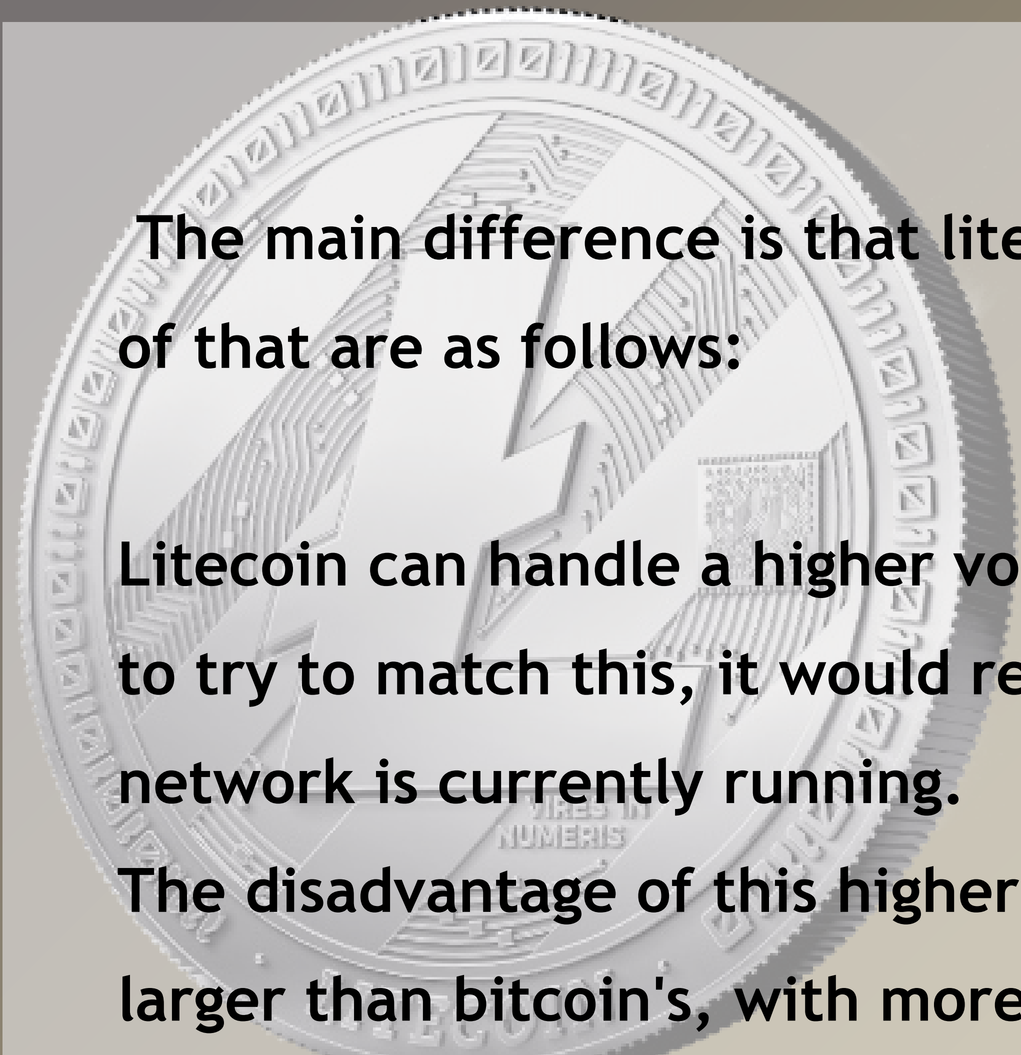
For the time being, 'state of the art' litecoin mining rigs come in the form of custom PCs fitted with multiple graphics cards (i.e.: GPUs). These devices can handle the calculations needed for scrypt and have access to blisteringly fast memory built into their own circuit boards.

There was a time when people could use GPU mining for bitcoin, but ASICs have made this method not worth the effort.



MorCryp

TRANSACTION DIFFERENCES



The main difference is that litecoin can confirm transactions must faster than bitcoin. The implications of that are as follows:

Litecoin can handle a higher volume of transactions thanks to its faster block generation. If bitcoin were to try to match this, it would require significant updates to the code that everyone on the bitcoin network is currently running.

The disadvantage of this higher volume of blocks is that the litecoin blockchain will be proportionately larger than bitcoin's, with more orphaned blocks.

The faster block time of litecoin reduces the risk of double spending attacks - this is theoretical in the case of both networks having the same hashing power.

A merchant who waited for a minimum of two confirmations would only need to wait five minutes, whereas they would have to wait 10 minutes for just one confirmation with bitcoin.

Transaction speed (or faster block time) and confirmation speed are often touted as moot points by many involved in bitcoin, as most merchants would allow zero-confirmation transactions for most purchases. It is necessary to bear in mind that a transaction is instant, it is just confirmed by the network as it propagates.

MorCryp