Litecoin

From Bitcoin

Contents

What is Litecoin?

Litecoin is an alternative cryptocurrency based on Bitcoin. It differs from Bitcoin in that it targets a faster block rate (2.5 minutes) and uses scrypt for the primary hashing done in mining. MtGox announced in April 2013 that they would add support for Litecoin trading, a plan that was delayed due to recent DDOS attacks.

While scrypt was claimed to be resistant to GPU-based mining early on, GPUs are currently the most efficient hardware with which to mine Litecoins. One of the aims of Litecoin was to provide a mining algorithm that did not compete with Bitcoin.

In April 2013, Litecoin reached a market cap of $70 million and achieved a network strength above 12 gigahashes/second. This compares roughly to a network strength for Bitcoin of 12 terahashes/second.

Differences from Bitcoin

Scrypt Proof of Work

Litecoin uses scrypt as a proof-of-work scheme. Scrypt adds memory-intensive algorithms to reduce the efficiency of the kind of parallelization that GPUs offered in early Bitcoin mining. This led to Litecoin primarily being mined with CPUs at the beginning. CPU-based mining has been challenged by the appearance of more energy-efficient GPU-based mining around July/August of 2012 bringing a roughly ten-fold increase in network hashing strength. GPUs are currently the dominant Litecoin mining technology.

Scrypt has been less widely used and analyzed than the SHA2 hashing algorithm used in Bitcoin, so there is some concern about possible weaknesses in its cryptographic scheme being discovered in the future.

Faster Blocks

The Litecoin blockchain differs from Bitcoin in that it generates blocks every 2.5 minutes on average (four times Bitcoin's rate). This means that merchants who accept transactions only 1 block deep get that confirmation quicker. However, it should be noted that more blocks are required to achieve the same amount of confirmation strength as Bitcoin (6 blocks of litecoin are not equivalent to 6 blocks of bitcoin). Unfortunately, this increases the number of hashes that are wasted in mining since miners will be working from the non-best block more of the time.

84 Million Litecoins

Litecoin started with miners generating 50 coins per block as with Bitcoin, but to maintain Bitcoin's inflation rate chage schedule, the block reward gets halved every 840,000 blocks. As a result, the network is scheduled to produce a total of 84 million litecoins.

Different Addresses

Litecoin addresses start with L due to their version number. Otherwise, they are generated identically to Bitcoin

Litecoin addresses start with L due to their "version number". Otherwise, they are generated identically to Bitcoin addresses.

(Slight) Premining

Litecoin had two blocks premined, one more than the minimum single genesis block needed to start a block chain.

Criticism

Redundancy

Besides a faster first confirmation, Litecoin does not provide any other features over what Bitcoin provides. Because of this lack of innovation, some believe Litecoin is unlikely to match or surpass Bitcoin's value or user-base. It remains to be seen if the use of a different mining algorithm and faster block times add sufficient value for Litecoin's long-term survival.

Not Silver to Gold

Some argue that Litecoin cannot make sense as "silver to bitcoin's gold", because Bitcoin itself is both gold and silver: While in the long-run, the BTC unit may be too valuable for everyday trade ("gold"), there are other, much smaller units that can just as well serve the purpose of "silver" while being naturally/automatically "converted" to/from BTC.

Vulnerability to mining monopoly

Similarly to Bitcoin, Litecoin can be attacked by an entity that can match or exceed the hashrate of the network. Such a "51% attack" becomes more difficult to launch and maintain as the hash rate of the network grows. However, this argument posits that Litecoin is designed to be inefficient on all common computer components (both CPUs and GPUs) meaning that a malicious entity need only produce a small batch of specialized/custom hardware to overtake all the commodity mining systems combined.

Memory bandwidth refutation

Some attempt to refute this by arguing that scrypt is not designed to be inefficient, but is instead designed to be highly dependent on memory bandwidth. Since the high-speed cache RAM on modern processors already takes up most of the die space, no sizeable improvement could then be made by creating custom chips. If we accept this argument we then estimate the cost of attack utilizing GPUs that are avilable today.

To do so we start with an estimated cost of hardware at $400 per megahashes per second and the October 2013 Litecoin network hashrate of 30 gigahashes per second. The total amount of equipment necessary to match and takeover the Litecoin network via 51% attack is then an estimated $12M USD (or about 45,000 AMD HD 7950s).

Pump and Dump Scheme

According to some, one or more of the aforementioned reasons imply that Litecoin has no future potential, and therefore effectively functions as a "pump and dump" scheme (http://www.investopedia.com/terms/p/pumpanddump.asp) , rewarding those who get in sooner at the expense of those who adopt it just before it finally fails (and are left with nothing).

Additionally, people often complain that the Litecoin community misrepresents it in other ways, such as portraying "faster block times" as if it makes transactions faster, and scrypt as if it is resistant to ASIC or FPGA hardware, in order to pretend Litecoin has value and inflate its value.

It's important to note, generally these critics do not think that Litecoin/Blockchain currencies are pump and dump schemes "per se"; but rather that the existing network effect of Bitcoin, combined with the lack of meaningful differentiation between Litecoin and Bitcoin and Litecoin's adoption of a "designed to fail" proof-of-work algorithm; that Litecoin is bound to fail in the end. Bitcoin does not suffer from these "flaws" and therefore does not fall under the "pump and dump" scheme, according to this argument.

External links

- Litecoin website (http://litecoin.org/)
- Litecoin forum (http://forum.litecoin.net/)
- Litecoin block explorer (http://explorer.litecoin.net/)
- Charts (http://www.ltc-charts.com/)
- Litecoin network graphs (http://litecoinscout.com/static/)
- Litecoin wiki (https://github.com/litecoin-project/litecoin/wiki)
- Litecoin Global Exchange (virtual stock exchange) (https://www.litecoinglobal.com/)
- Crypto Street - Advanced Trading Exchange for Litecoins (http://www.crypto.st/)
- MIT Technology Review: Bitcoin Isn't the only Cryptocurrency in Town

(http://www.technologyreview.com/news/513661/bitcoin-isnt-the-only-cryptocurrency-in-town/)

See also

Cryptocoin