User:Iddo/Comparison between Litecoin and Bitcoin

Da Litecoin Wiki.
(Reindirizzamento da **Comparison between Litecoin and Bitcoin**)

Indice

SHA256 mining vs scrypt mining

For proof of work (https://en.bitcoin.it/wiki/Proof_of_work) , Bitcoin uses the highly parallelizable SHA256 (http://en.wikipedia.org/wiki/SHA-2) hash function, hence Bitcoin mining is an embarrassingly parallel (http://en.wikipedia.org/wiki/Embarrassingly_parallel) task. Litecoin uses scrypt (http://www.tarsnap.com/scrypt.html) instead of SHA256 for proof of work. The scrypt hash function uses SHA256 as a subroutine, but also depends on fast access to large amounts of memory rather than depending just on fast arithmetic operations, so it is more difficult to run many instances of scrypt in parallel by using the ALUs (http://en.wikipedia.org/wiki/Arithmetic_logic_unit) of a modern graphics card. This also implies that the manufacturing cost of specialized scrypt hardware (ASIC) will be significantly more expensive than SHA256 ASIC. Since modern GPUs have plenty of RAM, they do prove useful for Litecoin mining, though the improvement over CPUs is less significant than it was for Bitcoin mining (about 10x speedup instead of 20x speedup when comparing Radeon 5870 GPU to quad-core CPU). See Litecoin mining hardware comparison and Bitcoin mining hardware comparison (https://en.bitcoin.it/wiki/Mining_hardware_comparison) .

The particular scrypt parameters that Litecoin uses (N=1024,p=1,r=1) let non-mining users who run the full client (and thereby verify and propagate the blocks) multitask in their operating system without affecting the responsiveness. These scrypt parameter still reduce the advantage of ASIC by a 10-fold estimate, according to Colin Percival, the creator of scrypt[1][2].

See also: bcrypt in Cuda? (http://crypto.stackexchange.com/questions/400/why-cant-one-implement-bcrypt-in-cuda) , Why a GPU mines faster than a CPU (https://en.bitcoin.it/wiki/Why_a_GPU_mines_faster_than_a_CPU) , bcrypt (http://en.wikipedia.org/wiki/Bcrypt) (scrypt predecessor)

Pros

- The market entry costs for Litecoin mining are cheap, anyone with a computer connected to the internet can mine litecoins in order to make a profit and to sustain the Litecoin network. Even CPUs can be used to mine Litecoin, albeit less effectively than modern GPUs. The inexpensive market entry cost implies a decentralized mining power.
- There is a danger that some entities would make a large one-time investment in ASICs (http://en.wikipedia.org/wiki/Application-specific_integrated_circuit) and centralize the mining aspect of the Bitcoin network, i.e. the market entry costs for Bitcoin mining would become too expensive for most people (this assumes that the objective of those entities isn't to sell their ASICs on the market). The scrypt algorithm used by Litecoin ensures that lots of memory is needed per hash attempt, basically by using the input as a seed to fill a large amount of memory with a pseudorandom sequence (http://en.wikipedia.org/wiki/Pseudorandom_number_generator) , and then using another seed derived from the input in order to access this sequence at pseudorandom points while generating the output hash. Since memory is the resource of general-purpose computers which is the most expensive to reproduce for ASICs (in particular it's more expensive than ALUs), this means that a one-time investment in ASICs for Litecoin mining would be much more expensive [3]. The memory size parameter of scrypt was selected (originally by ArtForz and Lolcust) to fit into 128.5kB, so that it'd only utilize the L1/L2 cache (http://en.wikipedia.org/wiki/CPU_cache) and wouldn't hit the L3 cache and the RAM. This means that it's possible to participate in the Litecoin network without affecting system responsiveness and with no disadvantage in propagating the blocks on common hardware, while still requiring a significantly large amount of memory per hash attempt.
- Websites can easily embed a Litecoin miner so that casual visitors would be able to support the website by

contributing their spare CPU cycles while browsing (example (http://www.litecoinpool.org/embed)). Having OpenCL (http://en.wikipedia.org/wiki/OpenCL) access through web browsers in order to utilize the GPU of casual visitors is much more problematic.

- Developers who wish to gain advantage over regular miners might try to create implementations of scrypt that run better on specific types of hardware, which would advance the current state of knowledge in areas unrelated to Litecoin, e.g. password cracking by brute-force or dictionary attack.

Cons

- Attacks by botnets (http://en.wikipedia.org/wiki/Botnet) . If the botnet operator runs an unmodified litecoind in order to earn coins then such a botnet only attacks the computers under its control, not Litecoin itself, as it would actually strengthen the Litecoin network. However, the objective of a crypto-currency is to improve the world rather than to improve itself. Botnets with a high enough proportion of the total hash power could try double-spending (https://en.bitcoin.it/wiki/How_bitcoin_works#Double_spending) attacks on the Litecoin network.

- The resale value of CPUs/GPUs/FPGAs implies that miners don't necessarily have stake in the system, therefore greedy miners who participate in attacks against the network are more likely with Litecoin than with Bitcoin[4].

Faster transaction time

The difficulty (https://en.bitcoin.it/wiki/Difficulty) of Litecoin adjusts so that a block is generated every 2.5 minutes on average, instead of the 10 minutes average of Bitcoin.

Pros

- Many people are anxious to see their transaction confirmed in the blockchain as soon as possible.

- Greater granularity, for example merchants may wish to accept transactions with only 2 confirmations in Litecoin (5 minutes), while in Bitcoin you would have to wait at least 1 confirmation (10 minutes).

- Less expected time and variance until a miner earns his reward. For example, if the network consists of 1000 miners where each of them has an equal amount of hashpower, then an individual miner is expected to earn his reward after 1000 blocks on average, but waiting for 1000 blocks is 4 times faster with Litecoin compared to Bitcoin. This implies that it is easier to sustain a relatively small mining pool with Litecoin, hence Litecoin can potentially be more decentralized than Bitcoin.

- Waiting for the additional confirmations during about the same time period that's used with Bitcoin (e.g. 24 Litecoin blocks instead of 6 Bitcoin blocks) means that an attacker will start the gambler's ruin process[5][6][7] with a greater deficit, so the probability for a double-spending attack to succeed is smaller. To elaborate: assuming that SHA256 is a random function, the probability of successfully generating a block at each nonce attempt is constant and independent of all other attempts[8]. Now suppose for the sake of argument that it takes on average one year to generate a block, that an attacker named Alice has 20% of the total hash power, that an honest miner named Bob has the other 80% of the hash power, that a merchant named Carol waited for 4 confirmations i.e. about 4 years before sending the merchandise to Alice, and that during those 4 years Alice managed to generate 1 block (on average that's what we'd expect) in secret. So Alice and Bob now compete in the gambler's ruin game, with Alice starting the game with a deficit of 3 blocks, and having 1/5 chance of winning each round. Because all nonce attempts are independent, if Alice won the first round then all the work that Bob did in this round is disregarded, and Alice and Bob start the second round from scratch. For stronger security, Carol can wait for more than 4 blocks before sending the merchandise, so the initial deficit of Alice is expected to be higher, i.e. Bob can spare to lose more rounds and therefore the probability of Alice carrying out a successful double-spending attack is smaller. Intuitively, the stronger security is achieved because Alice has a better chance to defeat Bob in few rounds than in many rounds (because she's at a proportionate disadvantage in each round), so by forcing Alice to play more rounds before sending the merchandise she would need a higher proportion of wins during this confirmations period in order to stand a chance in the gambler's ruin game that follows (for example with 40 confirms and same 20% hash power she's expected to fork 10 secret blocks and have a deficit of 30 blocks, as opposed to 3 blocks). The average time of each round doesn't play a role in the analysis, the relevant parameters are the proportion between the hash power of Alice and Bob in each round, and the number of rounds that Alice has to win in order to overcome her initial deficit. So in case the average time to generate a block is e.g. one minute instead of one year, this analysis still holds, unless the 1min block time has detrimental effects on the honest miner(s) relative to the attacker (see cons).
    - Therefore, relative to Bitcoin the security may be enhanced for Litecoin users who wish to wait for the extra confirmations.

Cons

- More overhead, the blockchain becomes more bloated. Clients running in simple verification mode (https://en.bitcoin.it/wiki/Scalability#Simplified_payment_verification) will be affected the most: in simple verification mode the client stores only the block headers and current wallet balance, so 4x more storage space will be needed for Litecoin clients relative to Bitcoin clients running in this mode.

- Less security if everyone waits for a fixed amount of confirmations (e.g. 6 blocks), because the higher amount of work that honest miners spend on losing branches implies that relatively less computing power is being put to good use while generating the blocks, so it would be easier for a dedicated attacker to double-spend litecoins compared to bitcoins. To elaborate: let's assume network propagation time of 2 seconds, i.e. it takes 2 seconds for each node to broadcast the longest chain that it knows of to all other nodes. With 2.5min blocks, on average

for each node to broadcast the longest chain that it knows of to all other nodes. With 2.5min blocks, on average once every 150 seconds some node broadcasts the valid block that it found, so during the 2 seconds of propagating the new block, the other miners are wasting their hash power while working on a shorter chain, which implies that 2 out of 150 seconds are being wasted on average. If there's a fork where different groups of miners work on different chains of same length then that's ok, i.e. they don't dilute the overall hash power, and if different groups of miners work on forks of different lengths then they'll switch to the longest chain after the network latency interval. So in total 2/150 of the honest hash power is being wasted, i.e. 1.33% dilution, compared to 10min blocks where 2/600 is 0.33% dilution.
    - This analysis is incomplete because it only takes into account the dilution in hash power of the honest miners, and not the fact that when the blockchain forks more frequently it means that an attacker (with no hash power) could scan the network and try to double-spend by broadcasting inconsistent transactions to the competing chains. However, the probability of a fork (by the honest miners) to persist diminishes exponentially with the length of the forked chains. Therefore, a merchant can take precautions either by waiting for more confirms, or by scanning the network and looking for an attempt to double-spend the transaction that he received .
    - Waiting for the same fixed amount of confirmations means that even if the probability of carrying out a double-spending attack isn't much higher than with slower blocks, the cost of carrying out the double-spending attack is cheaper: generating 6 blocks of 2.5min difficulty requires 4x less hash power compared to generating 6 blocks of 10min difficulty. So an attacker could afford more double-spending attempts[9]. Though in the case of an attacker with less than 50% of the hash power who competes against a network in which merchants wait for a greater number of confirmations (for example 12 Litecoin confirmations instead of 6 Bitcoin confirmations), the expected cost of a successful double-spending attack would be higher in comparison to the network with the slower blocks, since the success probability of the attack decreases exponentially with the amount of confirmations[10].

- Another security risk arises with attacks that rely on network partitioning, for example if Europe and America lose internet connectivity then an attacker could spend his coins in both continents. The relevant parameter in these scenarios is the absolute time until all nodes have enough time to communicate with each other, not the frequency of generated blocks. Therefore, this isn't an inherent problem of the protocol, because waiting for 4 times the amount of blocks relative to Bitcoin would be adequate, or in other words the problem lies in the default amount of confirmations.

- If the number of transactions increases by an extremely large factor, it will require more computational power to validate an increased number of ECDSA signatures at each block. With fast blocks, doing this validation in time could potentially be a problem: if there's a non-negligible probability that the time to find a nonce which generates a valid PoW is shorter than the time to validate all the ECDSA signatures in the block, then an attacker can gain an advantage over honest miners by purposely generating blocks that include fewer transactions (currently an attacker has very little to gain by trying to generate empty blocks, and one relevant effect is that the coins that he earns could become less worthy because their market value drops due to this attack).

See also: Myth - Point of sale with bitcoins isn't possible because of the 10 minute wait for confirmation (https://en.bitcoin.it/wiki/Myths#Point_of_sale_with_bitcoins_isn.27t_possible_because_of_the_10_minute_wait_for_confirmation)

Difficulty retarget

The retarget block is 2016 in both Bitcoin and Litecoin, but because Litecoin blocks are found 4 times faster, the difficulty will retarget about every 3.5 days.

Pros

- When the computation power of the network reduces dramatically in the event that many miners suddenly quit, block generation would crawl until the next difficulty adjustment. Having a faster retarget mitigates this concern.

Cons

- Shorter retarget window may lead to less stable difficulty adjustments. For example, if a proportionally high amount of CPU power connects to the Litecoin network only during Sundays, not having any of that CPU power inside a 3.5 days retarget window will cause the difficulty to vary. Unstable difficulty is bad if it doesn't reflect the hash power of the network accurately: when the difficulty is too low relative to the CPU power that is currently in the network, the faster blocks imply more overhead, less security (see previous section), and more monetary inflation, and when the difficulty it too high relative to CPU power, the slower blocks mean slower transaction time.

- Unstable difficulty might encourage chain hopping.

- Less security from attacks that rely on lowering the difficulty. Example: an attacker makes a one time investment in hash power, uses this hash power to start extending a recent block with his own fork of consecutive blocks while lowering the difficulty (easier to do with the shorter retarget window), isolates a node of e.g. some online bank from the rest of the network, waits until his fork is longer than what this node has already seen in the real blockchain, broadcasts his forked chain to this node, and with the lower difficulty he now needs less hash power to continue to communicate with the isolated node until it agrees to transact in the forked chain[11].

Total number of coins in existence

The total number of litecoins that will come into existence is 4 times the total number of bitcoins that will come into existence, 84 million compared to 21 million. The initial reward for each Litecoin block is 50 litecoins. The rate of

existence, 84 million compared to 21 million. The initial reward for each Litecoin block is 50 litecoins. The rate of litecoins generation is halved every 840,000 blocks, i.e. 4 times more blocks than with Bitcoin. Because Litecoin blocks are generated 4 times faster than Bitcoin blocks, this means that the monetary inflation of Litecoin follows the same trajectory as that of Bitcoin[12][13], so for example at the year 2020 around 3/4 of all litecoins will have already been generated.

Since the total money supply of Litecoin is 4 times greater than the total money supply of Bitcoin, it implies that if 1 litecoin becomes worth more than 0.25 bitcoins then the market cap (http://en.wikipedia.org/wiki/Market_capitalization) (and hence purchasing power (http://en.wikipedia.org/wiki/Purchasing_power)) of Litecoin will be bigger than the market cap of Bitcoin, under the (probably incorrect) assumption that roughly the same fraction of litecoins and bitcoins were destroyed due to users losing their secret cryptographic keys.

Bug fixes

- Time warp bug[14]: the Bitcoin difficulty calculation is off by one block, so an attacker can repeatedly try to generate the last block of each retarget window, and use a fabricated timestamp of 2 hours into the future in order to make the time difference from the first block in the retarget window high, thus lowering the difficulty by 0.5%. Because of the bug, the bogus timestamp isn't used as the first block in the next retarget window, and therefore the 2 extra hours aren't being compensated for in the next difficulty calculation. Once the difficulty is low, the attacker can mine many fast coins, or in the case of a small chain, an attacker with 51% hash power could reduce the difficulty to 1 and mine a new fork from the genesis block. This isn't a feasible attack on Bitcoin, because the probability of repeatedly generating the last block once every 2 weeks at such high difficulties is negligible. Although fixing this issue in Bitcoin is possible, it should be done carefully (by adding rules that encourage nodes to upgrade over time) so to avoid a chain fork, i.e. old clients who didn't upgrade might operate with another difficulty and therefore disagree regarding which blocks are valid. In Litecoin this bug is fixed[15].

Conclusion

One possible way to view Litecoin is as silver to Bitcoin's gold, in the sense that it is a relatively less valuable cryptocurrency that is easier to obtain and transact with. The properties that make Litecoin fit to accomplish this purpose can be summarized as follows:

- Transactions are 4 times faster than with Bitcoin, in exchange for less conservative and possibly weaker security guarantees (depending on human behavior).
- CPU/GPU mining means that the barriers to entry into the Litecoin mining market are cheap relative to Bitcoin mining.
- The total amount of litecoins is 4 times higher than the total amount of bitcoins.

References

1. ↑ Colin Percival comments on Litecoin scrypt (http://bitbin.it/7bmKZqTx) .
2. ↑ Colin Percival on #litecoin-dev 02 (http://bitbin.it/E68HeKkM) .
3. ↑ Tarsnap: The scrypt key derivation function (http://www.tarsnap.com/scrypt.html) .
4. ↑ https://bitcointalk.org/index.php?topic=327064.msg3513617#msg3513617
5. ↑ S. Nakamoto, Bitcoin: A peer-to-peer electronic cash system (http://www.bitcoin.org/bitcoin.pdf) , 2008.
6. ↑ M. Rosenfeld, Analysis of hashrate-based double-spending (https://bitcoil.co.il/Doublespend.pdf) , 2012.
7. ↑ http://en.wikipedia.org/wiki/Gambler's_ruin
8. ↑ https://bitcointalk.org/index.php?topic=5521.0
9. ↑ https://bitcointalk.org/index.php?topic=51504.msg615442#msg615442
10. ↑ https://bitcointalk.org/index.php?topic=260180.msg2783389#msg2783389
11. ↑ https://bitcointalk.org/index.php?topic=46498.msg556137#msg556137
12. ↑ https://en.bitcoin.it/wiki/Controlled_Currency_Supply
13. ↑ http://en.wikipedia.org/wiki/Bitcoin#Monetary_differences
14. ↑ https://bitcointalk.org/index.php?topic=43692.msg521772#msg521772
15. ↑ GitHub: Fix zeitgeist2 attack thanks to Lolcust and ArtForz (https://github.com/litecoin-project/litecoin/commit/b1be77210970a6ceb3680412cc3d2f0dd4ca8fb9) .