Lite Coin White Paper

Litecoin is the result of some of us who joined together on IRC in an effort to create a real alternative currency similar to Bitcoin. We wanted to make a coin that is silver to Bitcoin's gold. Various alternative currencies have come and gone. Some brought innovation, but they all had problems.

Litecoin is a peer-to-peer Internet currency that enables instant, near-zero cost payments to anyone in the world. Litecoin is an open source, global payment network that is fully decentralized without any central authorities. Mathematics secures the network and empowers individuals to control their own finances. Litecoin features faster transaction confirmation times and improved storage efficiency than the leading math-based currency. With substantial industry support, trade volume and liquidity, Litecoin is a proven medium of commerce complementary to Bitcoin.

Blockchain

The Litecoin blockchain is capable of handling higher transaction volume than its counterpart - Bitcoin. Due to more frequent block generation, the network supports more transactions without a need to modify the software in the future.
As a result, merchants get faster confirmation times, while still having ability to wait for more confirmations when selling bigger ticket items.

Wallet Encryption

Wallet encryption allows you to secure your wallet, so that you can view transactions and your account balance, but are required to enter your password before spending litecoins.
This provides protection from wallet-stealing viruses and trojans as well as a sanity check before sending payments.

Mining Reward

Miners are currently awarded with 25 new litecoins per block, an amount which gets halved roughly every 4 years (every 840,000 blocks).
The Litecoin network is therefore scheduled to produce 84 million litecoins, which is 4 times as many currency units as Bitcoin.

Open Source Software
Litecoin is an open source software project released under the MIT/X11 license which gives you the power to run, modify, and copy the software and to distribute, at your option, modified copies of the software. The software is released in a transparent process that allows for independent verification of binaries and their corresponding source code.

- ixcoin - Nasakioto premined 580k coins. Seemed like a pump and dump. Competed with Bitcoin for GPU resources - Dead (~2 gh/s)
- i0coin - Basically ixcoin without the premine. Not much support was given to this coin after it was released. - Dead (~5 gh/s)

Lite Coin White Paper

- SolidCoin - Innovative quick transaction times. Appears to have been run aground by CoinHunter, its creator, due to insecure changes and immature forum presence. - Dead, shutdown by CoinHunter
- GeistGeld - Lolcust premined 7.7 million coins. 15 second block time is probably a bit extreme. - Alive, but limping (~15 gh/s)
- Tenebrix - Lolcust premined 7.7 million coins. CPU proof of work using scrypt is very innovative. Price doing fairly well on btc-e.com. - Alive (~0.003 gh/s)
- Fairbrix - Basically Tenebrix without the premine. First launch was crippled due to bad config. Relaunch attacked initially - Doing OK now, but no exchange so far. - Alive, but limping (~0.0001 gh/s)

We wanted the best innovations of Bitcoin and these other currencies to create a coin with all of their benefits, but nearly none of their problems.

Proof of Work

We really liked Tenebrix's Scrypt proof of work. Using Scrypt allows one to mine Litecoin while also mining Bitcoin. We humbly offer a big thanks to ArtForz for the implementation.

Premines

Litecoin will come with 150 premined coins: just the genesis block and the first 2 blocks to confirm the genesis is valid. We believe a coin needs to be released in a fair manner. Having one person (or a group) control a large amount of coins that can be used as they see fit is against the decentralized vision of Bitcoin. Yes, it is true that without a stash of premined coins, we will not be able to afford to pay for bounties, but we believe people will see the virtue of this coin, invest in it as early adopters, and will be willing to spend time creating services to make this coin better.

Fast transactions

We were impressed by the convenience of SolidCoin's fast transactions. Although we know that fast confirmations are not necessarily as secure as Bitcoin's slower confirmations, they are very convenient for small merchants who don't need transactions to be super secure. The average Litecoin block takes 2.5 minutes, one quarter of Bitcoin's 10 minutes. So if merchants wanted to be as safe as Bitcoin, they can wait for 4 times the number of Litecoin confirmations as compared to Bitcoin. But most merchants can readily accept 1-confirmed transactions for small amounts of litecoins.

Difficulty retarget

We will keep the retarget block the same as Bitcoin's 2016, but because blocks are found 4 times faster, difficulty will retarget about every 3.5 days. The combination of fast retarget times and Scrypt proof of work (Litecoin will not compete with Bitcoin for miners) means we expect to not see the sort of problem Namecoin encountered; hashing power that leaves more suddenly than it came, causing a high difficulty slog for everyone who stayed.

Coin generation

Miners will generate 50 coins per block. In light of our faster blocks, to properly mimic

Lite Coin White Paper

Bitcoin's generation trajectory, we needed to change the blocks at which coin generation is halved. Bitcoin generation is halved every 210,000 blocks. Litecoin generation will be halved every 840,000 blocks. For those of you doing the math, Litecoin is scheduled to produce roughly 4 times as many coins as Bitcoin, about 84 million litecoins.

Fairness

We have come up with a plan that we believe is most fair. Some previous coins were released without Windows binaries or without source code; we consider this as unfair as it is unsafe.

We released the source code and binaries ahead of time... 3 days before launch. People had time to compile the source and run the client on their machines against the Litecoin testnet. So people were able to make sure everything was working well before the launch. We also had a poll so that people can vote for a launch time that best suits them. At the time of the launch (Oct 12 03:00 GMT), we released the genesis hash and everyone started mining at the same time. All it took was a simple change in the config file in order to mine the real coin instead of the testnet coin.

51% attack

The problem with alternative currencies is that the network hashrate is likely low when the coin starts up, making an easy target for any potential 51% attacker. With a little hope, a little prayer, a lot of hype, and due to our innovative release, there was a large hashrate from minute one. We believe this deterred any attackers from targeting this chain. As expected, there was a lot of natural orphaning of blocks, due to having so many people mining on the chain at once. With block locking at every difficulty change, we were able to avoid any attacks from succeeding. (if there were any)

Source code

The source code is here:
https://github.com/litecoin-project/litecoin

This is based on the latest Bitcoin code. You can either build the daemon version (litecoind) or you can build the gui version (Litecoin QT). See the build docs.

Similar to Bitcoin, you may want to create a litecoin.conf file here:
Windows: C:\Documents and Settings\<username>\Application Data\Litecoin
Win7: C:\Users\<username>\AppData\Roaming\Litecoin
Mac: ~/Library/Application Support/Litecoin
Unix: ~/.litecoin

Port is 9333. Open if on your router if you know how. This will allow you to have more than 8 connections.
And default RPC port is 9332. This is the port miners will use to communicate with your client/daemon.

Sample litecoin.conf file:

Code:

```
server=1
rpcuser=user
```

Lite Coin White Paper

```
rpcpassword=password

#Change this if you want to use a different rpc port for mining
#rpcport=9332

#Only uncomment this if you are running litecoind and want to run Litecoin in the
background (not Litecoin QT)
#daemon=1
```

See also Bitcoin white paper