# LitecoinPlus White Paper:
A Better Peer-to-Peer Electronic Cash System

Simone Lussardi
spider@litecoinplus.co
tysimon@litecoinplus.co
manomab@litecoinplus.co
support@litecoinplus.co
media@litecoinplus.co
http://www.litecoinplus.co
(git: https://github.com/Crypto-Currency/LitecoinPlus)

[**rev 1.10** – 2018-10-13 by tysimon]

Abstract. A purely peer-to-peer version of electronic cash to allow online payments to be sent directly from one party to another without going through a financial institution, while holding a more or less stable value. Basic project is derived from Bitcoin (BTC) software and Litecoin (LTC), has the same base structure and functionality, but it is an improvement under several aspects. First and foremost, LitecoinPlus team believes that PoW (Proof-of-Work, and related massive carbon print and power consumption) is destined to be left behind. It is no doubt necessary to maintain a fast moving network growing. The following charts clarify the evolution of LitecoinPlus:
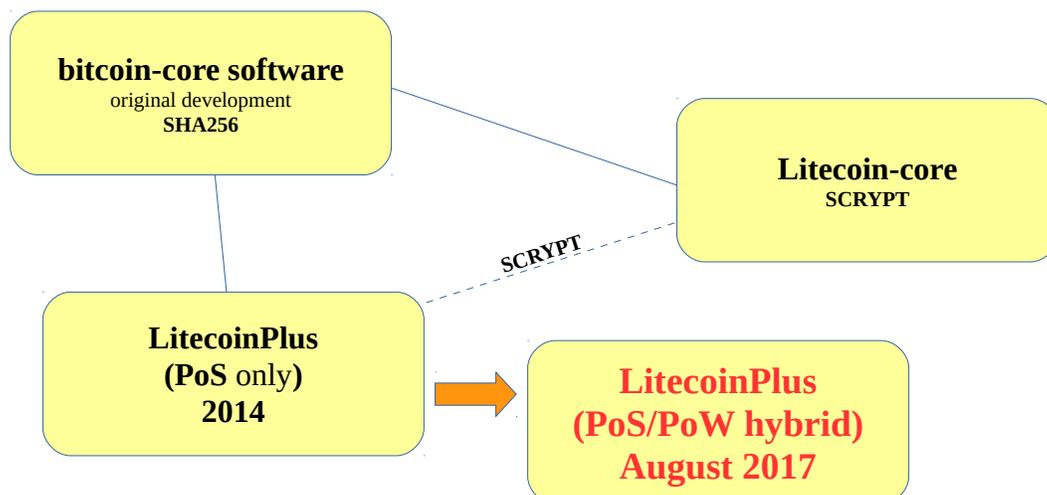
To put in graphical terms the fundamental differences between each of the above systems, here is a simple chart:
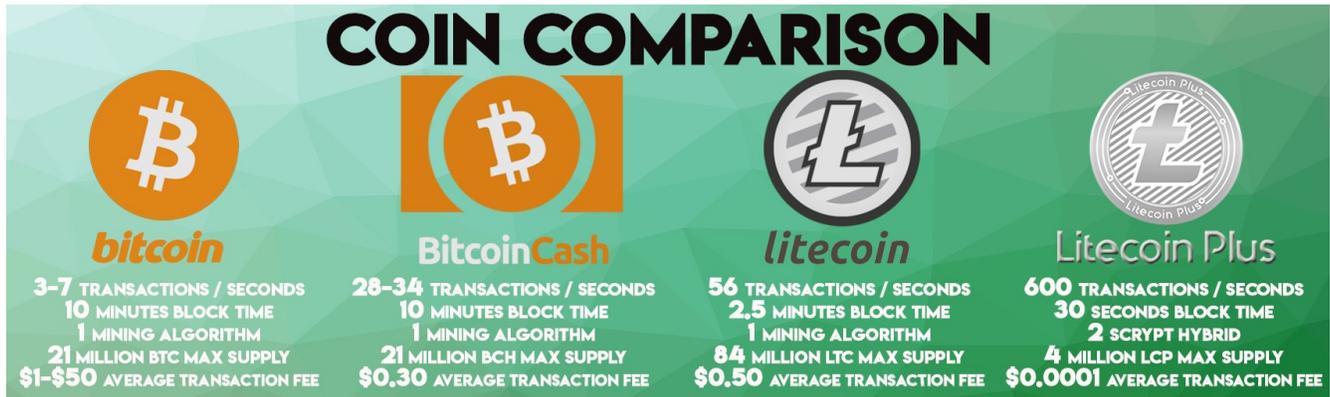
There is no need to re-invent the wheel and write down the specific of Bitcoin or Litecoin, since about everyone knows about those. If you are interested in the mathematics behind Bitcoin, block generation etc. (which applies fully to LitecoinPlus network as well), please refer to the original white paper of Satoshi Nakamoto: https://bitcoin.org/bitcoin.pdf. This white paper instead is about how we achieved the target mentioned above and how we plan to sustain it trough many years to come.

1. Introduction

LitecoinPlus has not started via an ICO (Initial Coin Offering). It was originally written as Proof of Stake coin exercise. "*Proof of stake (PoS) is a type of algorithm by which a cryptocurrency blockchain network aims to achieve distributed consensus. In PoS-based cryptocurrencies, the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e., the stake). In contrast, the algorithm of proof-of-work-based cryptocurrencies such as Bitcoin uses mining; that is, the solving of computationally intensive puzzles to validate transactions and create new blocks*" (*ref https://en.wikipedia.org/wiki/Proof-of-stake*). In contrast to the better known PoW, the non-computational, consensus nature of the algorithm make sure that power consumption is not an issue. PoS, when applied properly, can be run on any type of hardware, even very old computers just running the LitecoinPlus wallet software can generate enough blocks to sustain the network.

The fundamental issue of the first release of LitecoinPlus in 2014 was that it was a pure PoS coin, and as such an experiment. In order to sustain the network, a stable block generation is required (see later), which lead to the original LitecoinPlus network not able to sustain itself.

In the next page, we put some generic details on the specifications of LitecoinPlus.

GENERAL SPECIFICATIONS

Name: **LitecoinPlus**
Acronym: **LCP**
Encryption: **Scrypt**
Block generation: **Proof of Stake/Proof of Work hybrid**
Transaction time: **30 seconds**
Max supply: **4,000,000 coins**
RPC Port: **44350**
P2P Port: **44351**

Some resources for preliminary overview:

Main website: http://litecoinplus.co
Web wallet: https://wallet.litecoinplus.co
Stable git: https://github.com/Crypto-Currency/LitecoinPlus
Development/testing git: https://github.com/typhoonsimon/LitecoinPlus
Bitcoin Talk: https://bitcointalk.org/index.php?topic=2160325.0
Cryptocurrency Talk: https://cryptocurrencytalk.com/topic/87530-ann-litecoinplus-wallet-update-pow-added/
Twitter: http://twitter.com/Media_LCP
Discord community: https://discord.gg/wcZEb7Y

Proof of Work specifications

Start reward at 2 and reduce by .25 every 200,000 blocks, for a duration of roughly 9,6 years (1 block every 30 seconds is the global target)

Proof of Stake specifications

Interest rate: **15% annually**
Minimum coin age: **6 hours**
Maximum age: **30 days**

Compiling

Tested version: **3.3.2.9**

(* <u>only LTS versions, fully updated systems</u>)
(** <u>all versions are fresh installs, other combination of libraries may **not** work</u>)

OS	*Install sequence (depen.)*	*Server*	*QT*

Ubuntu 12.04 32/64	`sudo apt-add-repository ppa:bitcoin/bitcoin`
	`sudo apt-get update`
	`sudo apt-get install libdb4.8-dev libdb4.8++-dev`
	`> broken (precise support removed from bitcoin/bitcoin ppa)`
	`> can use another version of Berkeley, but this will broken`
	`compatibility, so is strongly not recommended`
		Obsolete	Obsolete

Ubuntu 14.04 32	`sudo apt-get install build-essential`
	`sudo apt-add-repository ppa:bitcoin/bitcoin`
	`sudo apt-get update`
	`sudo apt-get install libdb4.8-dev`
	`sudo apt-get install libdb4.8++-dev`
	`sudo apt-get install libboost-all-dev`
	`sudo apt-get install git`
	`sudo apt-get install libssl-dev`
	`sudo apt-get install libqt4-dev`
	`git clone https://github.com/Crypto-Currency/LitecoinPlus.git`
	`cd LitecoinPlus`
	
	`:::QT`
	`qmake USE_UPNP=-`
	`make`
	
	`:::d`
	`make clean`
	`cd src/`
	`make -f makefile.unix USE_UPNP=-`
	`strip ./litecoinplusd`
		Fully tested	Fully tested

Ubuntu 14.04 64	`[exactly same as 14.04 32]`	Fully tested	Fully tested
Ubuntu 16.04 32	`[exactly same as 14.04 32]`	Fully tested	Fully tested
Ubuntu 16.04 64	`[exactly same as 14.04 32]`	Deep tested	Deep tested
Ubuntu 18.04 64	`[exactly same as 14.04 32]`	Ongoing	Ongoing
Debian (all versions)	`[procedure to be defined]`	Ongoing	Ongoing
Windows XP	`[just run the setup software]`	Fully tested	Fully tested
Windows 10	`[just run the setup software]`	Fully tested	Fully tested

"Fully tested" sequence (qt means graphic version, d means server version):

1. Start the software (-qt or d) completely fresh, creates all the files, start syncing properly. After a while shutdown. Start again, can start and continue where it left off.
2. Replace the folder with existing data folder (for respective bits), start the software, make sure it can run properly.
3. Staking on -qt version
4. Transferring coins from/to other wallets
5. PoW mining on -qt and d version
6. Alternating between -qt and d versions
7. Partially import a bootstrap file, then continue via the network
8. Easily maintaining in sync once fully synced (no stuttering)
9. Long time stability (<u>no freezes</u>, <u>no abrupt terminations</u>)

"Deep tested" sequence:

1. <u>All of the above sequence</u>, plus the following items:
   1. Import completely a bootstrap file successfully.
   2. PoS mining on -qt version
   3. PoW mining on -qt and d version

2.   Bitcoin: areas of improvement

Bitcoin has forever changed the world view on how "value" can be exchanged, opening an entire new area into the crypto-currency world. As the first of anything, great innovation was brought to us by very fact of the market capitalization it achieved today.

Having said that, Bitcoin has a few points that prevent it from becoming widespread as a quick payment method:

- **Confirmations take a long time**: on average, payment confirmation may take up to 1 hour to get trough. This has made Bitcoin to be essentially used as a trading commodity only instead of allowing online payments.
- **Transfers are expensive**: given the popularity and price increase, transaction fees have become particularly expensive for Bitcoin.
- **Energy intensive**: getting the Bitcoin network going and the necessary block generation is an expensive business.

LitecoinPlus has improved on all the above points, with careful planning of the revised release in August 2017.

3.   Hybrid concept

As the original failure has shown, a pure PoS network is not able to sustain itself, especially at the beginning. Since there was no ICO and no initial coins (except for those generated in the initial stages of the tests), it was impossible to get the amount necessary to get the net going. For this reason, PoW was reintroduced, with a gradual "phase out" scheme, as below:

- **Original tests**: reward of 2.00 LCP per block, plus transaction fees
- **Block # < 2,000,000**: reward of 1.75 LCP per block, plus transaction fees
- **2,000,000 <= Block # < 2,200,000**: reward of 1.50 LCP per block, plus transaction fees
- **2,200,000 <= Block # < 2,400.000**: reward of 1.25 LCP per block, plus transaction fees
- **2,400,000 <= Block # < 2,400.000**: reward of 1.00 LCP per block, plus transaction fees
- **2,600,000 <= Block # < 2,400.000**: reward of 0.75 LCP per block, plus transaction fees
- **2,800,000 <= Block #**: reward of 0.50 LCP per block, plus transaction fees

This reward, combined with a block generation target of 30s, will be used to calculate the following two parameters:

- PoS difficulty
- PoW difficulty

The aim of these two parameters is to balance out new block generation, and achieve the target specified of 30s. Blocks are publicly readable at: http://lcp.altcoinwarz.com/
At the top of the block explorer, real time PoW and PoS difficulty, current supply and Bitcoin price are available.

4. Mining in details

Because LitecoinPlus has a hybrid bloc generation, mining takes place in two separate ways:

1. **PoS Mining**
2. **PoW Mining**

Regarding **PoS Mining**, it can be done by anyone on any type of hardware. It is recommended to have a stable Internet connection. The way of block generation is as following:

1. The wallet confirmed balance must be >= 0
2. If the wallet is encrypted, upon start it needs to be unlocked for staking (the icon indicating the staking status will report about this, and the wallet can be safely unlocked by going to menu **Wallet → Unlock To Stake...**).
3. Unlocking to stake is safe, the wallet will still need to be unlocked if any send transaction is required.
4. The algorithm will then mature coins for staking.
5. When the wallet is actively staking, the staking icon will turn green.
6. When a stake is generated, the following will happen:
   1. The transaction will appear in Overview and Transaction pages as unconfirmed
   2. The block that staked is divided into two, and one part is put into stake status (not spendable)
   3. When it starts to get confirmations, by hovering the mouse on the transaction, you can see the number of confirmation received
   4. When it received 3 confirmations, the block reward is **confirmed** but **not spendable** yet.
   5. When it matures 50 or more confirmations, the related reward become spendable and the stake amount is released, so it can mature again.

This is the calculation code for the PoS Mining reward:

```
int64 GetProofOfStakeReward(int64 nCoinAge, unsigned int nBits, unsigned int nTime, int nHeight)
{
  int64 nRewardCoinYear;
  if(nHeight < STAKE_FIX_BLOCK)
  {
    nRewardCoinYear = MAX_MINT_PROOF_OF_STAKE;
  }
  else
  {
    nRewardCoinYear = MAX_MINT_PROOF_OF_STAKE2;
  }
  int64 nSubsidy = nCoinAge * nRewardCoinYear / 365;
      if (fDebug && GetBoolArg("-printcreation"))
      printf("GetProofOfStakeReward(): create=%s nCoinAge=%"PRI64d" nBits=%d\n",
          FormatMoney(nSubsidy).c_str(), nCoinAge, nBits);

    return nSubsidy;
}
```

Regarding **PoW Mining**, any equipment that can handle SCRYPT algorithm mining (cpuminer, cgiminer or ASIC miners such as AntMiner L3+, InnoSilicon A4+ etc.) can be used for LitecoinPlus mining. As difficult increases, CPU or GPU mining is not profitable using anything else than ASIC miners. The Principle is as follows:

1. With given difficulty (block target = 30s), ASIC miners will generate shares
2. When a block is found, the block is submitted to the network via RPC
3. If accepted, the block will appear in the wallet as unconfirmed
4. Once 3 confirmations are received, the block is marked as confirmed, and the reward as immature, going to the immature balance, thus **not spendable**.
5. After **50 or more blocks**, the amount becomes mature and thus **spendable**.

Here below is the code calculating the PoW reward:

```
int64 GetProofOfWorkReward(int nHeight, int64 nFees, uint256 prevHash)
{
    int64 nSubsidy = 0 * COIN;

    if(nHeight == 1)
    {
        nSubsidy = 221400 * COIN;
        return nSubsidy + nFees;
    }


  if(nHeight > POW_RESTART_BLOCK)
  {
    nSubsidy= 2 * COIN;
    if(nHeight > POW_RESTART_BLOCK+200000)
    {
      nSubsidy = 1.75 * COIN;
    }
    if(nHeight > 2000000)
    {
      nSubsidy = 1.5 * COIN;
    }
    if(nHeight > 2200000)
    {
      nSubsidy = 1.25 * COIN;
    }
    if(nHeight > 2400000)
    {
      nSubsidy = 1 * COIN;
    }
    if(nHeight > 2600000)
    {
      nSubsidy = .75 * COIN;
    }
    if(nHeight > 2800000)
    {
      nSubsidy = .5 * COIN;
    }
  }
    return nSubsidy + nFees;
}
```

For all mining, expect some orphans to happen occasionally, especially for PoS mining, since not all the blocks will be able to make it into the network, especially if they are generated very close to each other (within a few seconds).

5. Coin control and Dusting

Because of the nature of PoS Mining, and block split, it's just a consequence that the number of blocks that build up the wallet balance will exponentially increase over time. This problem may become an issue for the user for two reasons:

1. When attempting to send a big amount, if the balance is built up by many tiny blocks, the sending function may fail even though the balance is enough.
2. The smallest fraction of coin is 8 decimals (0.00000001, for instance). When the block become so small that the related stake reward is less than that, the wallet will not stake anymore.

To resolve the above issue, the user has two options:

1. Using the Advanced Coin Control features (**not recommended** for normal users), the user can recombine his/her own coins into single larger block, so they will stake again.
2. Using the automatic Dusting function the internal algorithm will just optimize the blocks so that the wallet can continue to fairly stake and sustain the network, while not causing problem to the user. In order to dust:
   1. Select a destination address (**only own addresses can be chosen**)
   2. Press the "**Dust now**" button

In either cases, it may appear that after dusting, the wallet stake "*less than before*". As per frequency this is true, but the amount at the end of long period is exactly the same, if not more.

Here below is a sample page of the Dusting function, simply press **Dust now** button:

Amount	Date	Label	Received with	Confirmations
0.00009	18-06-03 10:39	(change)		10196
13.66	18-06-03 12:25	[DUSTING]		9879
13.674646	18-06-03 12:25	[DUSTING]		9879
15.61	18-06-05 10:02	[DUSTING]		76
15.625589	18-06-05 10:02	[DUSTING]		76
45.71	18-06-04 12:32	[DUSTING]		4740
45.71	18-06-04 12:47	[DUSTING]		4687
45.71	18-06-04 07:29	[DUSTING]		5809
45.71	18-06-04 12:06	[DUSTING]		4845
45.71	18-06-04 08:02	[DUSTING]		5711
45.71	18-06-04 12:28	[DUSTING]		4782

Found 30 blocks to compact.

| Refresh | Dust now |

6. Dusting over the server version

The dusting functionality is not available and should not be provided in the server version, and here's why. The function shall be attended by the user, to verify that the coins are confirmed once sent to self address. If confirmations are not received, actions need to be taken immediately to repair the wallet (using the Check/Repair or even ZAP commands), so that the coins are not lost.

But still, Exchanges and Mining Pools, even though they do not stake, they still need the dusting functionality, because when block number become large enough, and some user withdraw large amounts, the sending function may fail, leading to lots of problems for the tech support of that Exchange/Pool.

For the above reason, in order to safely dust your Exchange/Pool wallet, do the following procedure:

1. Setup a maintenance station with QT version of the wallet
2. Maintain this version synced from time to time, use an empty wallet or a temporary wallet while syncing (**not** the main wallet)
3. Make sure **reservebalance=9999999** is set into the LitecoinPlus.conf file of the QT wallet !
4. Put in stop the daemon of the main server
5. Copy out and backup the wallet.dat file
6. Using the graphical page, Dust your wallet
7. Follow the easy instructions on screen
8. Wait for all confirmations to appear after finishing the dusting, substantially making sure that all your balance appears as available in your Overview page.
9. Close the QT wallet properly.
10. Copy back to the real station's data folder
11. Start the process again and let it sync
12. Use RPC Console to make sure the balance is correct and available

7. Maximum supply

One of the target being the stable value, the maximum supply of coins is limited to 4,000,000 coins. Once that amount is reached, the software will not generate any more reward. The reward for generation of blocks will come exclusively from transaction fee. By then (we estimated roughly 10 years) the amount of transaction will be enough and the value would have risen to an amount that will sustain the network.

8. PoS and staking

In order to get the PoS going, the wallet need to have coins in it. A wallet with zero coins does not stake, thus it doesn't generate any blocks nor rewards. Once a positive balance is in, coins will need to "mature" in order to start generating rewards. It is all part of the internal algorithm to decide what blocks/coins mature and stake. The guaranteed annual return for staking is about 15%.

9. Reaching *all* users

LitecoinPlus has considered carefully all kind of users, from the IT expert to the non-expert. For this reason, a comprehensive structure of wallets have been devised, as following:

- **Software wallet**: the software wallet is the only one capable of generating blocks, in combination with mining equipment or stand-alone. Several versions are available:
  - Windows version
  - Mac OS version
  - Linux versions
    - QT version (litecoinplus-qt, intended for Linux graphical interface users)
    - *d* version (litecoinplusd, intended for mining professionals and exchanges)
- **Web wallet**: easily accessible via web, it is already active and running at https://wallet.litecoinplus.co. This makes it accessible to a large audience.
- **Android wallet**: even more easy than the web wallet, it's available on Google Play at the following page: https://play.google.com/store/apps/details?id=com.fitbobcat.litecoinplus

While all software flavors are basically the same, their behavior slightly differs. For example, when installing the daemon "d" version for exchanges or mining portals, the staking functionality needs to be disabled, otherwise funds cannot be transferred (see "PoS and staking"). In the next page, there is a chart displaying how the single-tier network of LitecoinPlus works with the respective type of wallets.

Relationship between the single-tier cloud and the user experience

LitecoinPlus
(single-tier cloud)
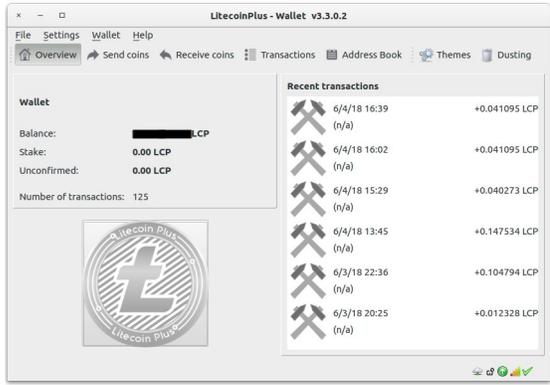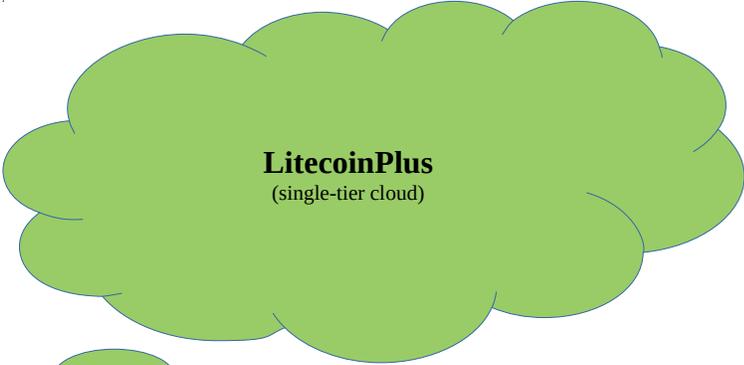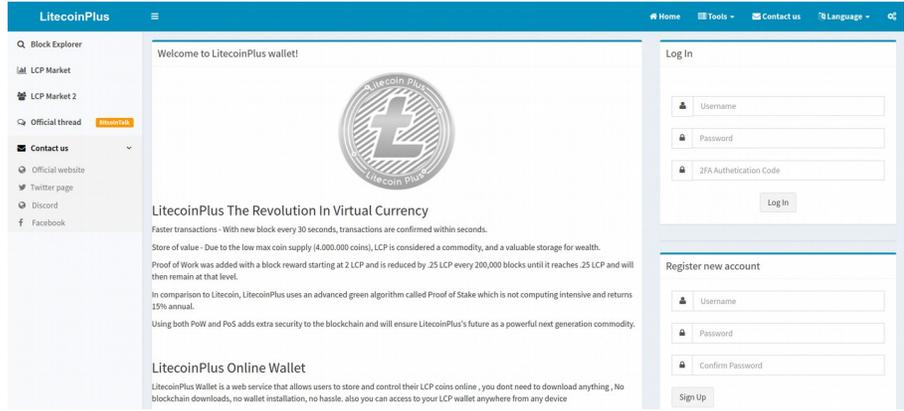
Wallet software

Web Wallet

Android Wallet

The advantages of the above solutions are obvious, and all aimed at simplifying the user experience. For those more advanced users who prefer to own their coins into their devices, the traditional wallet software is always available.

10. Software architecture

With its latest version 3.3.0.2, the wallet control has established the following principles and philosophy for its architecture and development:

1. **Database engine Berkeley DB (currently 4.8)**: contrary to the majority of other wallets, even popular ones like Bitcoin and Litecoin, we believe the extreme solidity and reliability of Berkeley DB is not worth the change. Most of them has migrated to LevelDB. LitecoinPlus uses Berkeley DB to store the blockchain index, the wallet, peer addresses and other information. LevelDB is reportedly:
   1. Quite buggy
   2. Project abandoned about 1 year ago
   3. More prone to file corruption than Berkeley DB
2. **Simple structures for speeding process**: where necessary, and following the growth of the network, simple improvements to keep the software going at the right pace, like the drastically reduced bulk operation at boot time, optimizations around the code and smooth network operation.
3. **Maintaining backward compatibility**: since the protocol is quite well defined and stable, there's no need to re-invent the wheel. Backward compatibility is of the utmost importance, because no developer, no matter how good, is infallible. A small bug could compromise the functionality and create a dangerous network split. We will strive with all forces to guarantee no network splits.
4. **Be ready to upgrade**: by choosing strong, portable bases (Berkeley DB, QT Framework), we are ready to go to the next step when used versions become obsolete and is time to upgrade.
5. **Keep the tools for repair**: LitecoinPlus wallet is one of the few that still keeps the wallet Check/Repair/ZAP tools. These tools are extremely helpful when problems arise with the wallet (like a sudden power outage or system hanging, leading to abrupt shutdowns).

For the future development, that will take LitecoinPlus software into years to come:

1. **Dev base**: keep a solid and stable development base (2-3 fixed programmers), with occasional help coming from the community.
2. **Strong support**: first hand communication as much as possible between developer and end user, to overcome most difficulties and debug most situations, giving the best experience possible (**never** let the user feel abandoned !)
3. **Always looking for new technologies**: "*there are always people out there who make the wheel rounder than you*", and when they do, we will be ready to take advantage of that, with final user experience always as top priority.

11. Files structure

The data folder for the LitecoinPlus folder varies from one operating system to another, but the data structure herein is the same, here below is an example of a data folder's content (Linux OS):

Name	Size	Type	Modified
database	2 items	Folder	13:42
themes	4 items	Folder	May 22
bindex0001.dat	424.1 MB	Binary	22:01
blk0001.dat	731.5 MB	Binary	22:01
blkindex.dat	865.7 MB	Binary	22:01
db.log	2.9 kB	Text	10:01
debug.log	8.5 MB	Text	22:01
LitecoinPlus.conf	172 bytes	Text	May 28
peers.dat	288.3 kB	Binary	22:01
wallet.dat	237.6 kB	Binary	22:01
.lock	0 bytes	Text	May 3

- **./database**: contains the log files for the transactional Berkeley DB
- **./themes**: may or may not be present, depending on your OS (may be elsewhere) and contain the color/font themes of your wallet software.
- **bindex0001.dat**: this is the boot index file. Not critical. If corrupted, simply delete this file and restart the wallet. The wallet will recognize that the file is missing and it will re-index the blockchain.
- **blk0001.dat**: the blockchain file. Important but not critical, can be rebuild by a resync if corrupted or lost.
- **blkindex.dat**: the blockchain Berkeley DB index file. Goes in pair with the previous one.
- **db.log**: the DB error/info log file
- **debug.log**: the wallet DB error/info log file. May be useful to developers when encountering issues.
- **LitecoinPlus.conf**: may be present or not, depending on your installation. Normally is not necessary, unless you are an advanced user.
- **peers.dat**: contains the addresses of known peers. If the file is corrupted or missing, it will just be rebuilt at the next boot.
- → **wallet.dat** ← : this is the most important file of them all. It contains all your keys and public keys for receiving and mapping your coins. If you loose this file, you will loose all your coins. Backup this file frequently. More advanced users can also make a paper-wallet using the command line in the console (Help/Debug/Console).

12. LCPEXCHANGE.COM

With the aim to provide a complete experience to the user **and** share benefits with the community, LitecoinPlus have its own exchange in the pipelines. The project timeline is supposed to be as follows:

1. **End of January 2019**:   alpha release of the exchange website
2. **End of March 2019**:   beta release of the exchange website
3. **End of June 2019**:   exit the beta release, enter into official one
4. **Mid 2020**:   start considering additional listings

The website link already registered, and is available at:

* http://www.lcpexchange.com
* http://www.lcpexchange.net
* http://www.lcpexchange.org
* http://www.lcpexchange.info

LCPExchange also serves as node monitoring. All users running a full LitecoinPlus node 24/7, on a public IP address, can register it to their account in the exchange and increase their share of benefits from it. Full nodes are very important as they increase greatly the overall network security, transaction speed, reduce greatly the impact of any attack. Furthermore, each node can stake and earn LCP, helping block generation and randomness even further.

12.1. General concept of the exchange

The general concept of the exchange is very simple. The base "currency" will be LitecoinPlus, so it is theoretically the only currency that can never be unlisted by it, no matter what. At the beginning, listing requests will not be accepted, the bucket of crypto-currencies listed will be the following:

- Bitcoin (BTC)
- Litecoin (LTC)
- Dogecoin (DOGE)
- Bitbar (BTB)
- Litebar (LTB)
- BitcoinFast (BCF)
- Bitgem (BTG)
- Bitcoin-sCrypt (BTCS)
- Emerald (EMD)

FIAT currencies will not be accepted. We will re-evaluate this every year, to consider whether is necessary to have them or not, and update this White Paper.

At the time of writing this White Paper, eventual listing fees have not been decided yet. It is however convened among the LCP group that free listing may even be accepted from communities that are friendly toward LCP, but generally listings will require a fee. 100% of the fees generated by the listing will go toward LCP promotion. If that amount becomes significant, the rest will be devolved to charity.

12.2. That sharing benefit part…

LCPExchange is all about sharing and engaging the community. The concept behind it is fully non-profit, and all profits made will be shared among the users involved. The principle on which this is based is like below:

1. All fees from exchange, withdraws and deposits will be publicly displayed
2. After just remove the expenses, the earnings will be distributed to the users of the exchange (see fixed proportion below)
3. The proportion to which a user is entitled to get benefits is calculated using the following principles:
    1. How much LCP he keeps in the exchange (other cryptos are not counted)
    2. Whether he/she is running a full node to support the network (node must be registered, and uptime/health will be monitored)

Regarding the earnings distribution, it is decided that at the beginning it shall be 20% / 80%. This means that 20% is to be kept in the hands of the developers to pay for hosting fees and all related expenses. The remaining 80% will be distributed among all users of the exchange. Details of the formula for distribution is given in the following section.

12.3. Formula for benefit sharing

The sharing of benefits is done in crypto-currency. It may be done in LCP or any other of the crypto-currencies that are present in the system at the moment. The proportion of the payment is calculated as follow:

- **60%** is reserved for the users who are running a **verified** full node and have LCP in their accounts
- **40%** remaining is for the users who only have LCP in their accounts

So, let's assume some example with random data. Suppose the situation of the current profit for the overall exchange is as the following table, in 4 random cryptos:

Currency	Total earn	80.00%	Prop-60%	Prop-40%	To exch.
BTC	3.907625	3.1261	1.87566	1.25044	0.781525
LTC	40.149	32.1192	19.27152	12.84768	8.0298
LCP	2000.89525	1600.7162	960.42972	640.28648	400.17905
BTCS	2087.524	1670.0192	1002.01152	668.00768	417.5048

Total earn is the total earning in each respective currency, 80% is the proportion dedicated and shared among users. Prop-60% and Prop-40% are the amounts dedicated for the groups with/without certified running nodes respectively. To exch. Is the remaining 20% left in the exchange to cover the expenses.

OK now let's assume the following situation, and related earnings:

User	Full node?	LCP-stake	BTC	LTC	LCP	BTCS
usera	Y	8000	0.88266353	9.06895059	451.966927	471.534833
userb	Y	9000	0.99299647	10.2025694	508.462793	530.476687
userc	N	2000	0.07578424	0.77864727	38.8052412	40.4853139
userd	N	9000	0.34102909	3.50391273	174.623585	182.183913
usere	N	22000	0.83362667	8.56512	426.857653	445.338453
Total LCP at stake 60%:		17000	1.87566	19.27152	960.42972	1002.01152
Total LCP at stake 40%:		33000	1.25044	12.84768	640.28648	668.00768

*(the formula in each column is [(LCP-stake / Total LCP) * Prop-xx%])*

In the above example, usera gets 0.88266353 BTC + 9.06895059 LTC + 451.966927 LCP + 471.534833 BTCS. The payment happens in each crypto direcly credited to the user account. There is no fee or commission for this transfer, is completely uncharged. If we paid in LCP only, some people may argue that we may enormously benefit from pushing people to buy LCP, which in some jurisdictions is also illegal to do.

The proportions or the percentages may be subject to evaluation from time to time, but always will be decided by the group and written in an agreed White Paper before changing them.

The concept is that the system will, automatically and once a month, take a picture of the situation and automatically distribute the profits according to the above formula.

12.4. Current fees

At the moment of writing this White Paper, it is decided to have the following fees for deposit and withdrawal of cryptos:

Currency	Deposit	Withdraw (min/fee)	→ LCP com.	← LCP com.
LitecoinPlus (LCP)	0 LCP	10/0.000200 LCP	-	-
Bitcoin (BTC)	0 BTC	0.01/5% BTC	0.2%/0.2%	0.2%/0.2%
Litecoin (LTC)	0 LTC	1/5% LTC	0.2%/0.2%	0.2%/0.2%
Dogecoin (DOGE)	0 DOGE	15000/5% DOGE	0.2%/0.2%	0.2%/0.2%
Bitbar (BTB)	0 BTB	10/3.3 BTB	0.2%/0.2%	0.2%/0.2%
Litebar (LTB)	0 LTB	260/180 LTB	0.2%/0.2%	0.2%/0.2%
BitcoinFast (BCF)	0 BCF	2000/1450 BCF	0.2%/0.2%	0.2%/0.2%
Bitgem (BTG)	0 BTG	[not defined]	0.2%/0.2%	0.2%/0.2%
Bitcoin-sCrypt (BTCS)	0 BTCS	3000/2100 BTCS	0.2%/0.2%	0.2%/0.2%
Emerald (EMD)	0 EMD	4000/2800 EMD	0.2%/0.2%	0.2%/0.2%

[*NOTE: regarding the fees for the major cyrpto, they are based on the market situation. The spirit of LCPExchange is not to lock the user up into an investment, instead is to create a healthy growth environment for everyone. If the crypto-currency market crashes down all together, we may just allow the users to withdraw other currencies at low or even no fee*]

Regarding deposits, we do not charge any fees apart from the fees that your wallet charge when making the deposit itself. For withdrawals, the top currencies will get high fees in % per withdraw, while other less popular currencies will get around 20 USD equivalent, not in %. These fees will be updated constantly as the market changes. This high fees are necessary to avoid dumping at the own exchange. If dump does happen, at least the entire community can benefit from it, not only the dumper himself. The commission for the exchange is set at 0.2% each for the Buyer and Seller. These fees already include network fees for sending from wallet to wallet.

12.5. Software specifications

We have no plans on making this software available via git. The server architecture will be Debian 64 bits, with PHP 7.2 and MariaDB flavor or MySQL as database. Because the architecture is centralized, we will make possible to export raw data from certain tables for absolute transparency. All parts that does not involve compromising the security of the exchange.
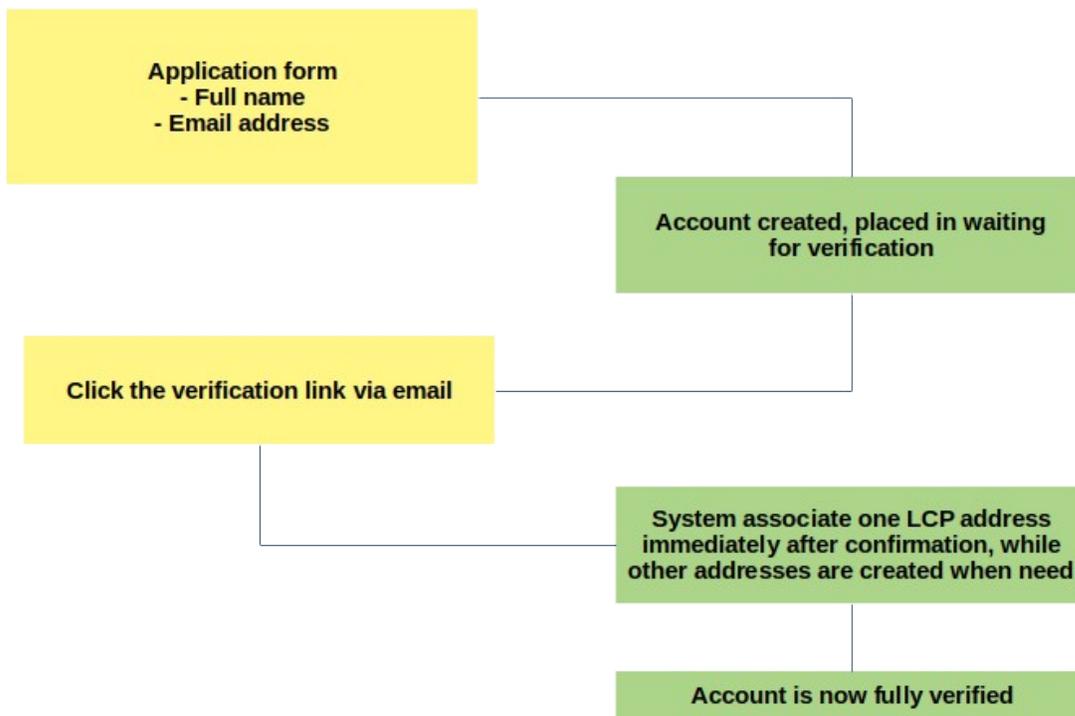
12.6. Security

The LCP daemon and exchange website will run on the same server, for greater security, with zero exposed ports online (except for http port 80 and https port 443). Other wallets' daemons are clustered via LAN into the main server, which then interfaces them via RPC. Other machines are not exposed via the Internet, except for those ports used by the wallet to sync the blockchain.

Enhanced rules and firewall protection for administration are put in place to avoid malevolent user reaching those precious interfaces.
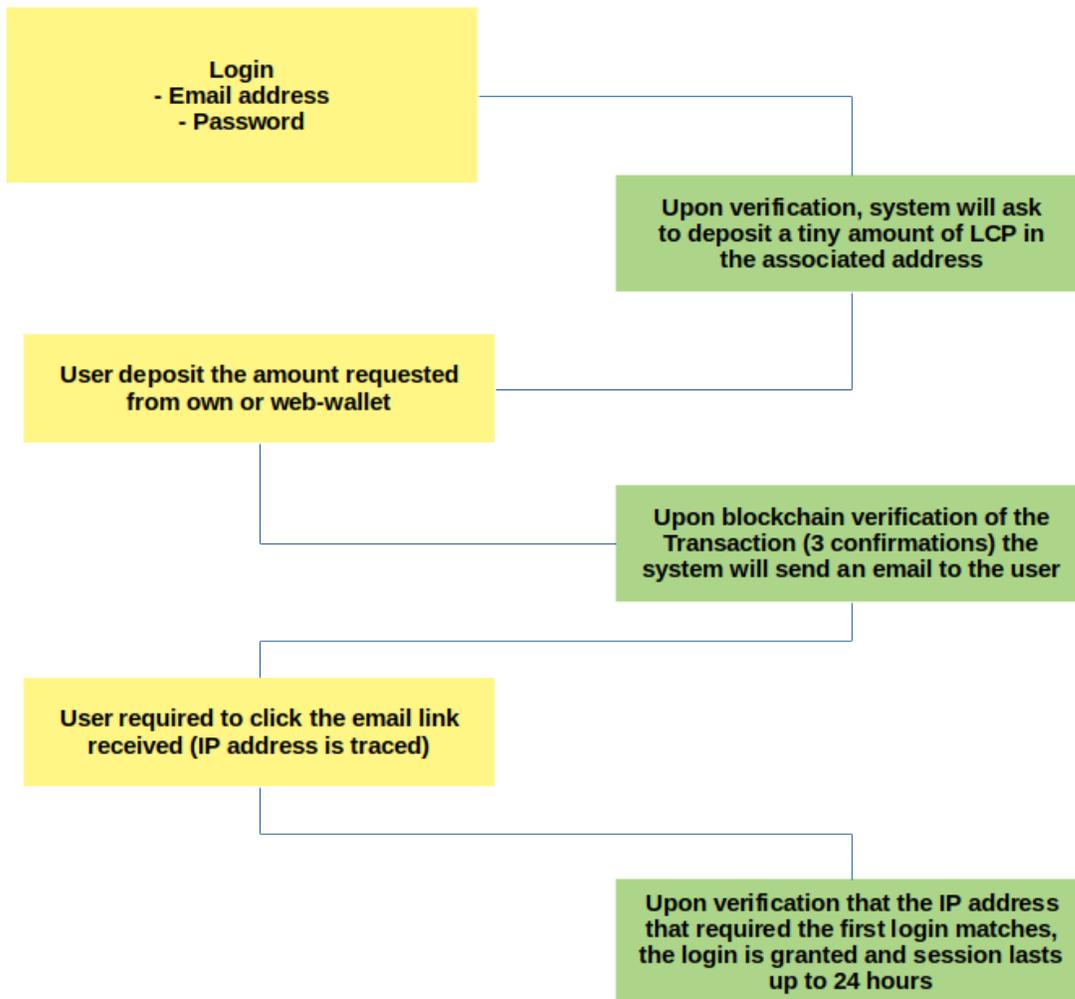
12.7. Account application

Regarding registration, the procedure will be pretty straightforward as usual for such kind of systems (no need to re-invent the wheel):

During the initial application, capctha is used to avoid robot and automated submissions.

12.8. Login

LCPExchange plans to implement a very innovative security method for logging in, all centralized around LitecoinPlus wallet, whether is the Web or Desktop version. Here are the details on how it works:

Login
- Email address
- Password

Upon verification, system will ask to deposit a tiny amount of LCP in the associated address

User deposit the amount requested from own or web-wallet

Upon blockchain verification of the Transaction (3 confirmations) the system will send an email to the user

User required to click the email link received (IP address is traced)

Upon verification that the IP address that required the first login matches, the login is granted and session lasts up to 24 hours

Because of the likely relatively large amount of cryptocurrency that will be stored in the exchange, this 3 step security implemented will guarantee sufficient safeguard against hacking attempts, in the following ways:

1. Basic security first step, with classic login attempt (user, password and captcha)
2. Enormous security feature by using the blockchain to confirm your transaction
3. Final confirm step from your email box, to make sure it wasn't other people that has actually abused of your username (plus the click has to happen from the same IP that has originated the request in the first place)

In order to crack this security, an hacker would need to get control of your account and your email address all at the same time.

12.9. Enhanced login version

LCPExchange even implements an enhanced login version activation, for the utmost security level: the user deposit has to happen from a defined address. Once this address is set, it cannot be changed anymore unless the user has the key of that address. This feature is not removable once applied, and should only be used by most experienced blockchain users.

X. MASTERNODES

Masternodes are used in special two-tier type currency, in which the layer of who-do-what is subdivided into two, and essentially the govern the background protocol of the network. For example, DASH is a two-tier network using Masternodes:

*"**Masternodes***
Unlike Bitcoin's single-tier network of miners, Dash utilizes a two-tier network of masternodes and miners.

As in Bitcoin, Dash miners secure the network by providing proof of work. The second tier of the Dash network consists of masternodes, which perform PrivateSend, InstantSend, and governance functions. In future releases aimed at improving ease-of-use, the masternode network will store encrypted data relating to user and merchant accounts (DashDrive), and will enable third party clients to interact with the Dash network via a decentralised API (DAPI)." (*ref* https://en.wikipedia.org/wiki/Dash_(cryptocurrency)#Masternodes)

LitecoinPlus is a single-tier network, and does **not** plan in the foreseeable future to become a two tier network, thus adding Masternodes. The well balanced combined capacity of PoS and PoW will suffice to make the network stable in the long run.