LITECOINZ

WHITE PAPER

The Revolution of Privacy

Fulfilling Satoshi's Vision for 2018 and Beyond

January 2018

Authors:

The LitecoinZ Community

HTTPS://LITECOINZ.INFO

Abstract

A better system is needed that removes the middlemen and empowers any two individuals to freely and securely transact. LitecoinZ is a low-fee, fast, and private transactional network. LitecoinZ is the product of a merger of Bitcoin with "Zerocash" protocol forked from ZCash.

It intends to offer a far higher standard of privacy through a sophisticated zero-knowledge proving scheme that preserves confidentiality of transaction metadata.

LitecoinZ has zk-SNARKs a peer reviewed privacy technology originally implemented by the Zcash Foundation. zk-SNARKs allows for provably anonymous and private transactions - an accomplishment no other privacy technology can claim. In conclusion this white paper will discusses LitecoinZ and its technological advantages.

Table of contents

Introduction

The “Right to Privacy” is essential to the cryptocurrency community. Privacy in the Financial world is critical in the digital currency community. There's still a problem with anonymous transactions on the block chains. Government and the private sector leverage massive datasets and machine learning to identify the individuals associated with a transaction. Lack of privacy in relation to Bitcoin and the original intent of its creator yet there exists a solution “**LitecoinZ**”.

A lot of cryptocurrencies have attempted to solve the privacy issue. Unfortunately many of these are capable of being compromised through various techniques due to their on chain transaction systems that promise anonymity. A research paper by MIT researchers discussed zero knowledge arguments of knowledge or zk-SNARKs. Cryptocurrencies that implement zk-SNARKs allow for shielded transactions funds are completely anonymous with no transaction or address balance appearing on the ledger. The researchers developed and launched Zcash the first cryptocurrency that incorporated zk-SNARKs. A founder’s tax was incorporated into the code of Zcash allowing the development team and early investors to collect 20% of coins mined by the community. LitecoinZ has no founder’s tax.

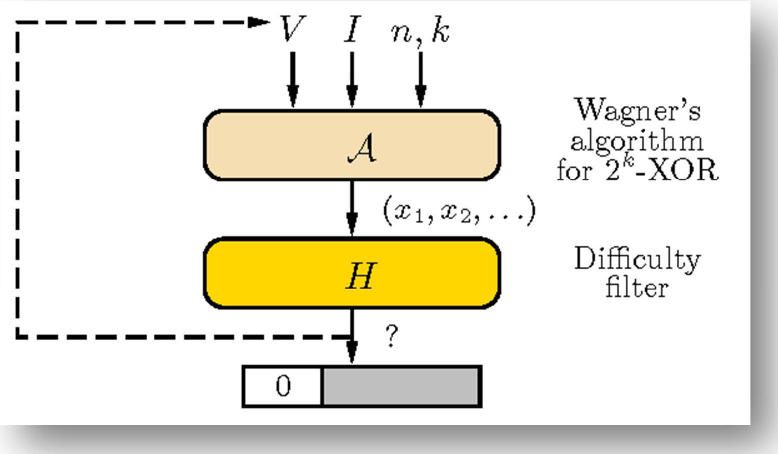
LitecoinZ Structure

LitecoinZ is based on Bitcoin technology with a Total Supply of **84 million coins** making the Supply 4 times bigger than Bitcoin or same size of Litecoin. Block reward of **50-LTZ** with a Block Size of 2 MB and halving every 4 years like in Bitcoin. LTZ uses the Equihash algorithm that brings Decentralization and zkSNARKs allowing Privacy for all users. With low Transaction Fees of 0.0001 LTZ.

Proof-of-Work: Equihash

LitecoinZ will utilize the Equihash PoW algorithm developed as a proof of work **POW** mechanism. Unlike other ASIC resistant POW algorithm Equihash is based on the **Birthday Problem** with the enhanced Wagner algorithm utilized to solve it. Equihash features memory hardness a steep computational penalty is associated with a reduction in memory usage and speed.

This feature increases the ASIC resistivity of Equihash due to the cost of implementing more memory into ASICs to make them competitive with GPU's or even CPU's.



Transparent And Shielded Transactions

Transparent transactions operate on the same principles as Bitcoin - input output and amount and signature. Sources of all funds destinations and amounts are stored transparently on the block chain. Shielded transactions conversely encrypt these details into a special section of a block called the JoinSplit. These transactions are verifiable but indecipherable to third-party observers.

When spending shielded notes the integrity of the block chain is kept via a specialized zero-knowledge proof algorithm called zkSNARKs.

This algorithm runs a series of computations to show the input values sum to the output values for each shielded transfer. Then a sender proves that they have the private spending keys of the input notes giving them authority to spend.

Private spending keys of the input notes are cryptographically linked to a signature over the whole transaction in a way that the transaction cannot be modified by a party who did not know these private keys.

Technical Specifications

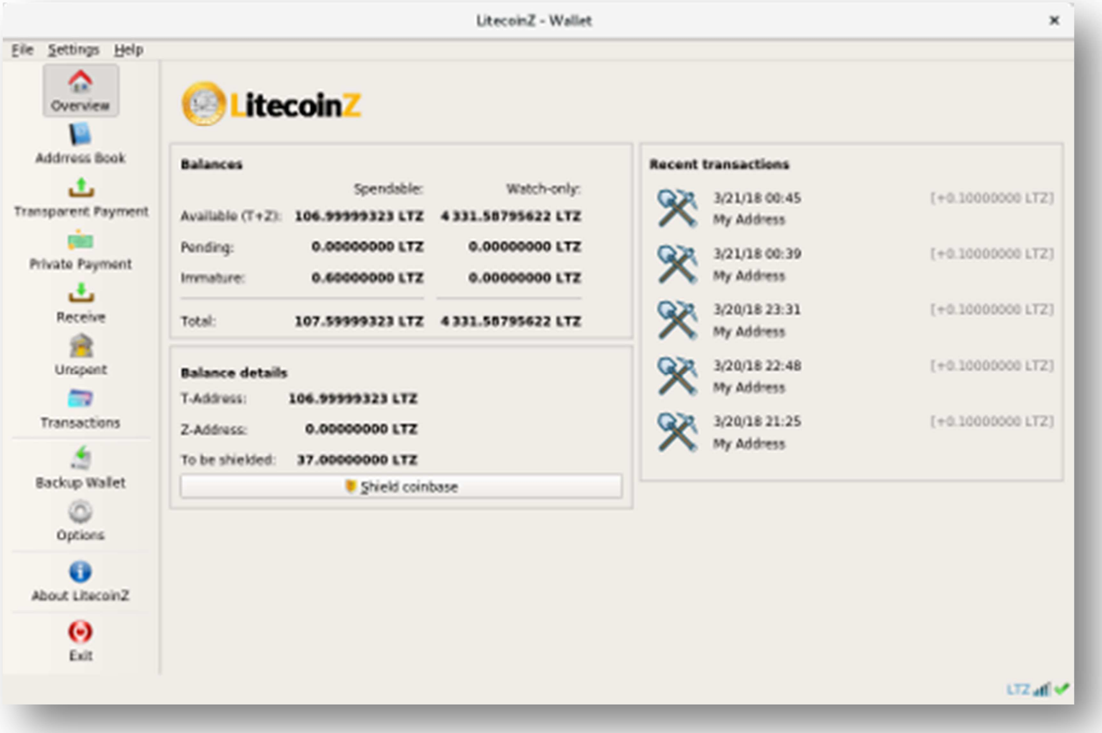
Coin Name	LitecoinZ
Coin Ticker	LTZ
Max supply	84 Million
PoW algorithm	Equihash
Privacy	zk-SNARKs
Block Interval	2.5 mins
Block size	2M
Block Rewards	50 LTZ
Block Rewards Halving	Every 4 years
Dev Rewards	No
Premine	5000 blocks
Mining Hardware	CPU / GPU
ASIC-resistant	Yes
Difficulty adjustment	Every block
Unique address format	Yes
Own signature	Yes
Own private key	Yes
Own public key	Yes
P2P Port	29333
RPC Port	29332

Decentralization

LitecoinZ implements a new PoW algorithm, Equihash, that makes mining decentralized again. Special computer hardware designed for LTC mining (ASICs) is obsolete for mining LTZ, giving ordinary users a chance to mine with ubiquitous GPUs.

Native GUI

LitecoinZ, is unlike many other arriving Zcash forks with one of the only Wallets with an Embedded native GUI that runs without 3rd party programs like java etc.. This gives the future development of LitecoinZ a convenient Codebase to maintain with a secure an more usable and reliable Wallet for the users. It's also Supported by the community and runs on: Windows/ Linux/ Mac OS. Mobile version Work in progress.



Balances

	Spendable:	Watch-only:
Available (T+Z):	106.99999323 LTZ	4 331.58795622 LTZ
Pending:	0.00000000 LTZ	0.00000000 LTZ
Immature:	0.60000000 LTZ	0.00000000 LTZ
Total:	107.59999323 LTZ	4 331.58795622 LTZ

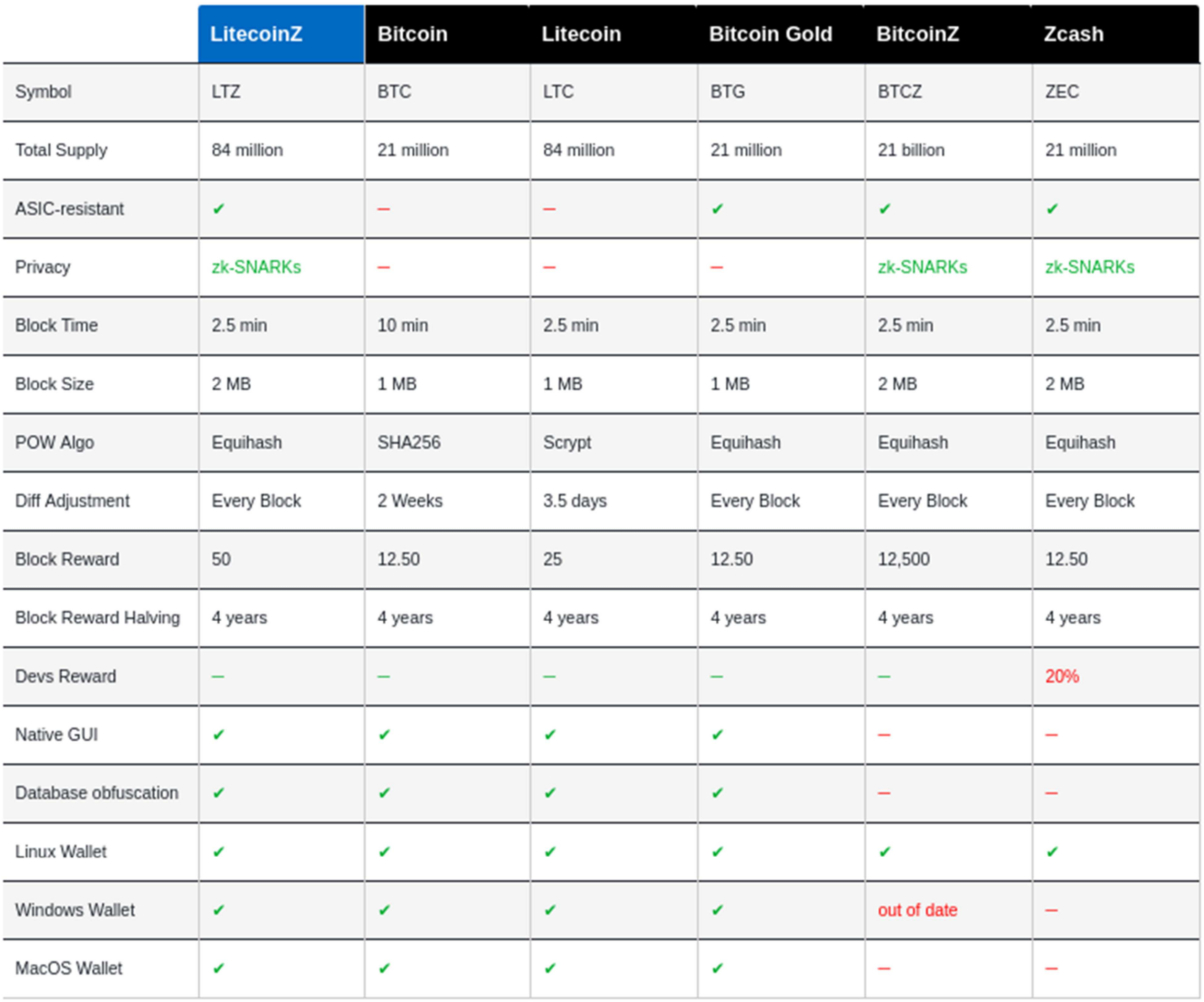
Balance details

T-Address:	106.99999323 LTZ
Z-Address:	0.00000000 LTZ
To be shielded:	37.00000000 LTZ

Recent transactions

3/21/18 00:45 My Address	[+0.10000000 LTZ]
3/21/18 00:39 My Address	[+0.10000000 LTZ]
3/20/18 23:31 My Address	[+0.10000000 LTZ]
3/20/18 22:48 My Address	[+0.10000000 LTZ]
3/20/18 21:25 My Address	[+0.10000000 LTZ]

Comparison Table



	LitecoinZ	Bitcoin	Litecoin	Bitcoin Gold	BitcoinZ	Zcash
Symbol	LTZ	BTC	LTC	BTG	BTCZ	ZEC
Total Supply	84 million	21 million	84 million	21 million	21 billion	21 million
ASIC-resistant	✓	–	–	✓	✓	✓
Privacy	zk-SNARKs	–	–	–	zk-SNARKs	zk-SNARKs
Block Time	2.5 min	10 min	2.5 min	2.5 min	2.5 min	2.5 min
Block Size	2 MB	1 MB	1 MB	1 MB	2 MB	2 MB
POW Algo	Equihash	SHA256	Scrypt	Equihash	Equihash	Equihash
Diff Adjustment	Every Block	2 Weeks	3.5 days	Every Block	Every Block	Every Block
Block Reward	50	12.50	25	12.50	12,500	12.50
Block Reward Halving	4 years	4 years	4 years	4 years	4 years	4 years
Devs Reward	–	–	–	–	–	20%
Native GUI	✓	✓	✓	✓	–	–
Database obfuscation	✓	✓	✓	✓	–	–
Linux Wallet	✓	✓	✓	✓	✓	✓
Windows Wallet	✓	✓	✓	✓	out of date	–
MacOS Wallet	✓	✓	✓	✓	–	–

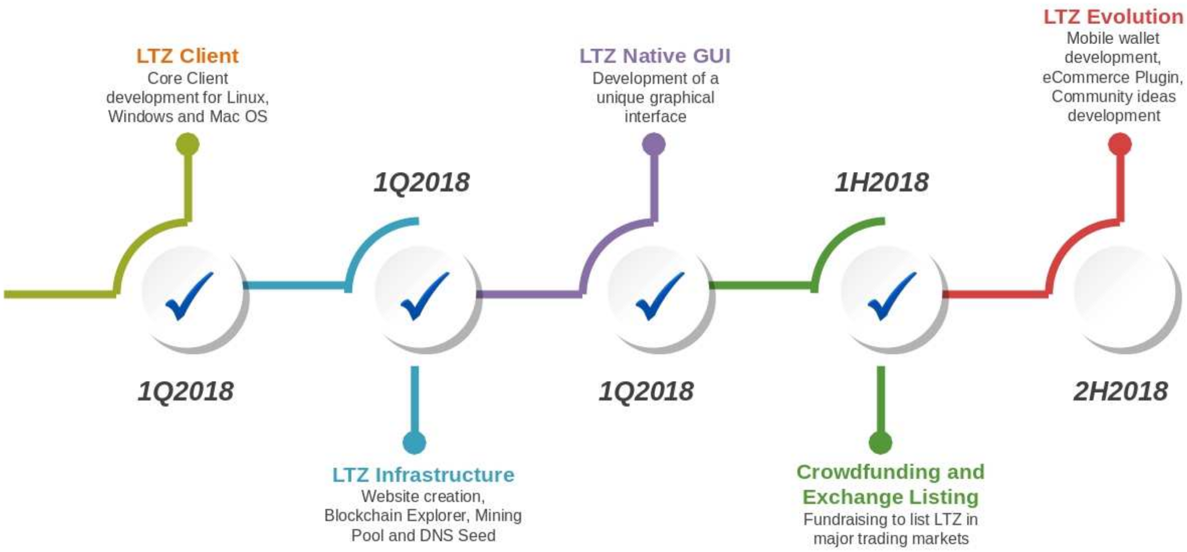
Transparency

LitecoinZ is a free open source software project that is built by volunteer developers and supported by a rapidly growing community that stretches across the globe.

Mining Rewards

Miners are currently awarded with 50 new LitecoinZ per block, an amount which gets halved roughly every 4 years (every 840,000 blocks).

Road Map


LTZ Client
Core Client development for Linux, Windows and Mac OS
1Q2018
LTZ Infrastructure
Website creation, Blockchain Explorer, Mining Pool and DNS Seed
1Q2018
LTZ Native GUI
Development of a unique graphical interface
1Q2018
Crowdfunding and Exchange Listing
Fundraising to list LTZ in major trading markets
1H2018
LTZ Evolution
Mobile wallet development, eCommerce Plugin, Community ideas development
2H2018