bitcoin-takeover.com

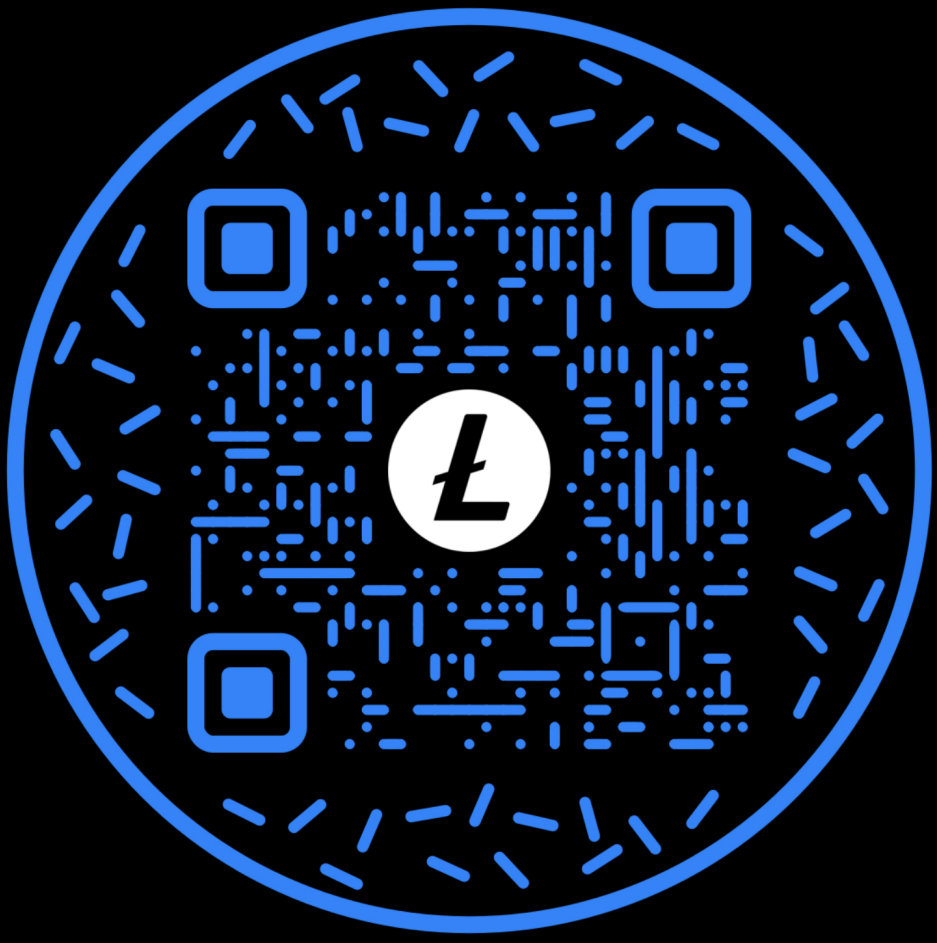
BTCTKVR

Litecoin edition!



FINANCIAL ADVISORY
LIFE-CHANGING CONTENT

Litecoin Foundation is a nonprofit organization dedicated to the adoption, awareness & development of Litecoin & its ecosystem.



LITECOIN Foundation

www.litecoin.net



Articles and Midjourney AI prompts to generate images (including covers):
Vlad Costea

Graphic editing and DTP design:
Leonard Luția (lutialeonard@gmail.com)

Bitcoin Takeover Podcast Season 15 graphics:
Mihai-Bogdan Dimache (michaeldimeart@gmail.com)

Litecoin Foundation ad design: Robbie Coleman
LayerTwo Labs ad design: Vlad Costea & Paul Sztorc
Bitrefill ad design: Mauro Peretti
Lokotech ad design: Ben Miklozek
Alephium ad design: Vladimir Moshnyager & Mikaël Vaivre
Lite.Space ad design: Indigo
Bitpay ad design: Leonard Luția

All AI-generated images are owned by Vlad Costea (and are free to use) under Midjourney's Content Rights.

This magazine will get published on **https://bitcoin-takeover.com/litecoin** under a Creative Commons license. Feel free to download it, distribute it, modify it, print it, and sell it. If you want to reward the original creator, send a donation to **ltc1q639d4ud84smx7s0zl7d2nas9aalgwpvetvc2m9**

TABLE OF CONTENTS

BTCTKVR LITECOIN EDITION



07 Why Litecoin?



11 How Litecoin Helps Bitcoin



14 Bitcoin vs. Litecoin. What are the differences?



17 Why is Litecoin so used in commerce?



20 The best Litecoin Wallets



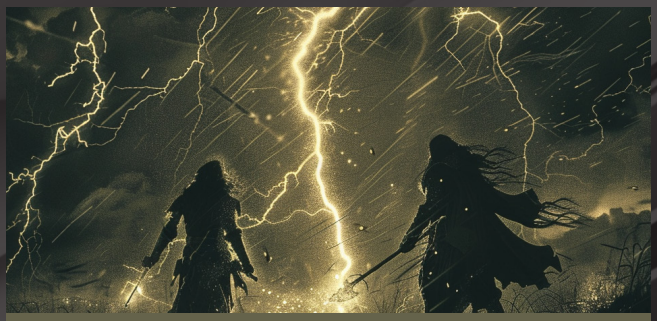
26 Interview with Paul Sztorc



30 How to run and use your own Litecoin Core Node



34 Charlie Lee quotes about MWEB, Litecoin & Privacy



36 Litecoin and the Lightning Network



38 The role of Litecoin in a Cypherpunk Future



42 Interview with Litecoin Devs



44 How to mine Litecoin and Dogecoin



51 Litecoin's MWEB What it is & how to use it



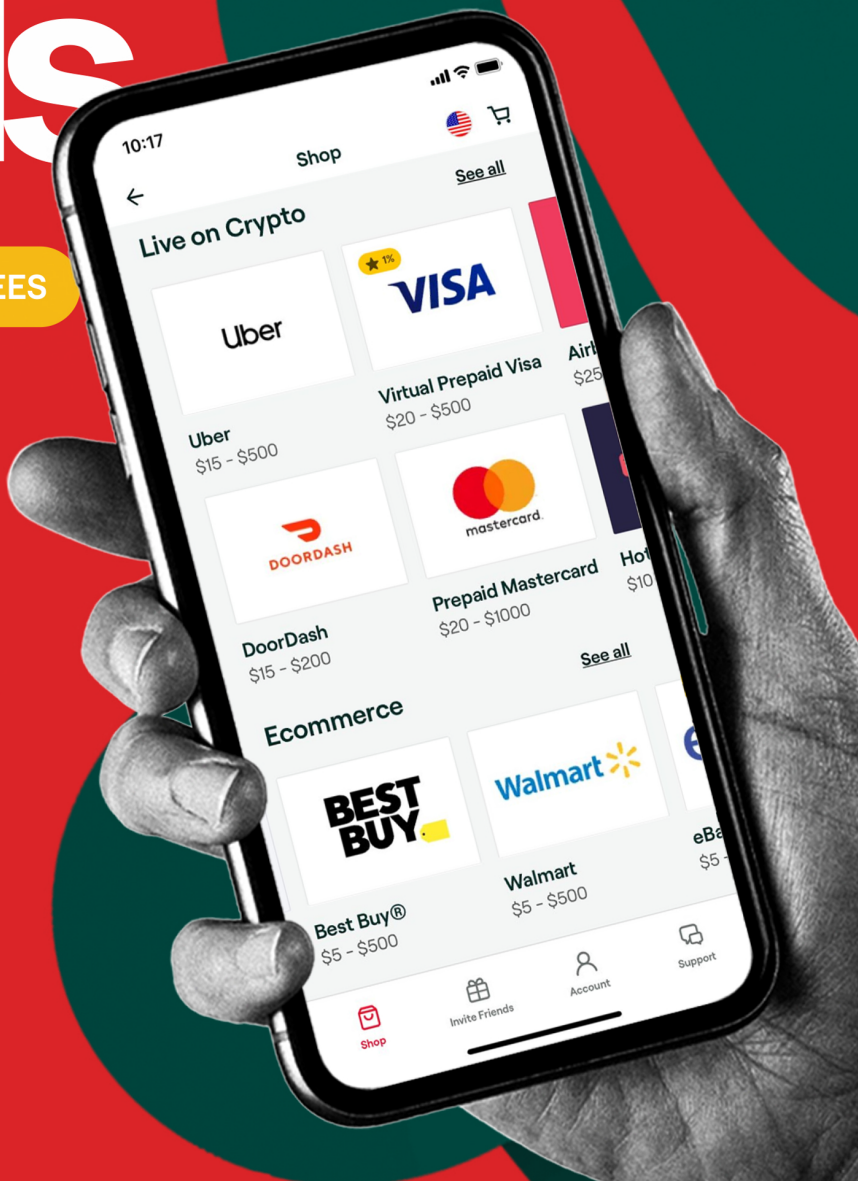
56 Litecoin and Drivechains

Bitrefill

Shop all of your favorite brands

USE LITECOIN NOT BANKS

ZERO FEES



bitrefill.com

Why Łitecoin?

"The Litecoin network is approaching its 13th year of existence."

As of July 24th 2024, the day of the 4th annual Litecoin Summit, the Litecoin network is approaching its 13th year of existence. For nearly 13 years, it operated without interruption and reliably allowed anyone around the world to make fast, secure, affordable, and provably decentralized financial transactions.

Litecoin was born in the middle of the bear market that lasted between 2011 and 2013, so it's no stranger to hard times: it was forged through fire, became the silver steel of a burgeoning industry, and went on to witness three more brutal bear markets. In between these moments of grief, which separated fundamentals from exuberance and inspired more improvements, there were glimpses of victory when Litecoin users felt like they were at the top of the world. But regardless of the price action, LTC was constantly used for payments — so the speculative side took the back seat to enable the medium of exchange to flourish.

Other coins came and went: they rose to prominence, had their moments in the spotlight, and then faded into obscurity never to recover. During this process, traders used Litecoin to get on and off exchanges — they leveraged the low fees, fast confirmation times, great transaction finality, and wide acceptance across exchanges in order to speculate on the new star. Sure, Bitcoin (and later Ethereum) were registering much higher transaction volumes. But when the fees became high, most traders came back to the good old Litecoin.

Over the years, sovereign individuals trying to live off of their cryptocurrency holdings would also benefit from Litecoin. Due to its similarity in design with Bitcoin, almost every BTC ATM offers the option to also buy and sell LTC. Furthermore, companies such as Bitrefill allow anyone to buy gift cards for popular stores, restaurants, hotels, and transportation networks using Litecoin. In the United States, Bitrefill even allows people to pay their bills with their LTC. This description barely scratches the surface, though: payments processors such as BitPay have thousands of integrations across businesses from all sectors, thus allowing Litecoin users to spend for virtually everything they may desire.

Even in Paralelni Polis, the first Bitcoin cafe in Prague, Litecoin is one of the only three forms of currency accepted (alongside Bitcoin and Monero). Speaking of Prague, the largest retail store in Czech Republic (Alza, the national equivalent of Amazon) accepts LTC payments for all of their products — through a European payments processor called Confirmo (formerly Bitcoin Pay, established in 2014). Therefore, it's safe to say that Litecoin's success in commerce is not only a North American affair that's mostly driven by businessmen such as Jon Moore and John Kim, or celebrities like Ben Askren. There's genuine organic growth that happened across 13 years and nobody can deny the proof of work behind it. Everyone who sought to avoid the banking system and needed fast settlement times and low fees could rely on the Litecoin network.





In 2014, three years into Litecoin's existence, the silver surfer has gained a new canine friend: as Dogecoin was facing the brutal reality of potential 51% attacks, Litecoin took it under under its Scrypt wing to allow the most popular Shiba Inu in finance to wave its tail and bark for as long as it pleases. The Doge didn't have a particularly prolific market performance until early 2021, when Elon Musk adopted him. Ever since that moment, Dogecoin has remained a solid contender to the top 10 coins and has also played a major role in keeping Litecoin miners profitable: since they can merge mine both LTC and DOGE, the revenue for the Proof of Work they provide is more significant and void of concerns. Litecoin saved Dogecoin, and then the king of shibes came back 7 years later to prove that he's much more than a good boy: he's the wow much coin.

Litecoin's journey was not without criticism and scrutiny: as bitcoiners converged towards currency and protocol maximalism, some of them referred to Litecoin as a cheap and pointless carbon copy. After the Lightning network and sidechains emerged on Bitcoin, it was said that altcoins such as LTC would die off. And when new and better marketed coins such as Terra Luna and Solana reached their peak, VCs like Mike Novogratz suggested that LTC should be removed from CNBC's price ticker. All of these opinions were proved wrong for different reasons.

Firstly, Litecoin was never just another carbon copy. There are multiple reasons why Litecoin survived for 13 years and continues to thrive, while nobody speaks of the other 2011 stars Peercoin, Namecoin, Terracoin, Devcoin, and Novocoin: it had a fair launch, the code was constantly maintained, and a community grew organically around it. Also, Charlie Lee coined (pun intended) one of the most memorable and lasting narratives in the space: Litecoin is the digital silver to Bitcoin's gold. While Namecoin was more different from a technological point of view, it didn't have such a powerful meme attached to it and the market action did not follow it.

Secondly, Litecoin has constantly played the role of a Bitcoin testnet with real incentives. While testnets are useful for developers, they are not made for demonstrating market demand and they don't attract hackers to try to break the code. Back in early 2017, when SegWit FUD was at its peak and critics would make ridiculous claims about its security ("SegWit coins are anyone-can-spend"), Charlie Lee negotiated activation with the Litecoin miners in order to prove the mightiness of Bitcoin's proposal. So Litecoin's activation of SegWit came in late April, almost 4 months before Bitcoin's. To prove the haters wrong, Reddit user throwaway40338210716 even set up a SegWit address with 40000 LTC in it (the equivalent of $1 million in early May 2017). Though the coins were moved to a different wallet in September of the same year, there was never any report of stolen coins or any complaint from the litecoiner. By that time, Bitcoin had also activated the exact same piece of code via soft fork. Plot twist: Charlie Lee revealed in October 2017 that it was him who set the bounty, then moved the LTC to another wallet when his demonstration was no longer necessary.

After the SegWit activation, companies such as ACINQ and Lightning Labs started experimenting on Litecoin. They knew that some mistakes were potentially too expensive to make on Bitcoin, so they used a chain that's 100% compatible and enables developers to port their code whenever it's provably safe and ready. This is why the first mainnet Lightning network transactions were broadcast on Litecoin and it took a few months for the exact same developments to come to Bitcoin. At the time, part of the vision for the Lightning network was to build atomic swap platforms between blockchains — so users could trade between BTC, LTC, and other LN-compatible chains without middlemen and by using protocols instead of businesses. Though there were some experiments, this idea never came to fruition... but maybe it was just a little too ambitious for its time.

Litecoin didn't really need SegWit and Lightning, as the base layer fees have always been low and the network never experienced significant congestion. However, Bitcoin did need them — so Litecoin took on the role of the live testnet with incentives and arguably played a historical part in helping users make up their mind about groundbreaking (but heavily criticized) developments. There's a lot of value in having financial bounties for new code, but some people take everything for granted: there's an entire roster of toxic Bitcoin maximalists who will argue that Litecoin is worthless and would most likely share this article across social media to call the author names such as "shitcoiner" and "grifter".

But as always, dogmas are rarely rooted in reality and the free market tends to always destroy narratives. The only





"Are you using Liquid with L-BTC? Good luck spending that anywhere..."

reply that someone like Francis Pouliot, Saifedean Ammous, or Giacomo Zucco would give is that "these coins only exist to fuel gambling and speculation, while a bunch of degenerates print their own money outside of the sacred 21 million to generate inflation". But in the year of 2024, Bitcoin still doesn't have a simple and non-custodial solution for people who can't afford to pay high on-chain fees.

Are you using Liquid with L-BTC? Good luck spending that anywhere... you're also going to need permission from the federation members to peg out (or else pay a percentage of the amount to a swapping service). Using custodial Lightning or ecash mints? Hopefully, the custodians will have mercy and never steal your funds in some epic rug pull (or the regulators won't seize their money). To this day, there are more ATMs, exchanges, and brick and mortar businesses which accept Litecoin (albeit, through payments processors) than Bitcoin on Lightning. This phenomenon doesn't happen because these businesses don't adhere to the Bitcoin maximalist thesis and therefore don't want to support Bitcoin's second layers — it's a matter of supply and demand, and Litecoin is here to deliver. The reality is that, as of July 2024, Bitcoin is still struggling with scaling and must implement better proposals for layer 2s.

Last but not least, it's worth noting that Litecoin is a forward-looking project. After activating SegWit and providing an excellent testbed for the Lightning Network, the developers didn't just rest on their laurels. They went back to work in 2018, in an attempt to give Litecoin the last missing property of sound money: fungibility. What started as a research to bring Confidential Transactions to Litecoin and grew into a potential collaboration with privacy coin Beam, eventually became MWEB: the marriage between Grin++ (one of the most popular implementations of the MimbleWimble protocol, written in C++) and Extension Blocks (a 2013 proposal by Bitcoin Core developer Johnson Lau, which sought to increase the block size without a hard fork).

To say that MWEB is a big deal is an understatement: through it, Litecoin has added a protocol-level way to get privacy for the sender, the receiver, and the amounts being sent. Furthermore, the upgrade doubles down as a block size increase which future-proofs the network for times of much higher demand... while once again showing the Bitcoin community how it's done. While it's true that MimbleWimble isn't the best of privacy protocols and isn't recommended for darkweb markets, it can receive further improvements through voluntary CoinJoins from users.

MWEB is definitely the future of Litecoin and the feature from which many killer apps can flourish. It's a bold move which marks a slight diversion from the Bitcoin path, but also a big step into the future.

And it's not like the improvements will end with MimbleWimble: as Charlie Lee hinted on S15 E34 of the Bitcoin Takeover podcast, Drivechains might be coming next to enable the creation of a sidechain for every popular use case. If this proposal gets activated, then everything from Ethereum contracts to Monero ring signatures can get ported 1:1 to be traded for LTC. While there's no guarantee that these miner-enforced sidechains will get traction, the research is certainly useful to once again combat some FUD. It might also increase the demand for LTC.

Such is a fate of Litecoin: not designed to directly compete, but to support Bitcoin in ways that are not possible on the mother chain or its valueless testnets. If there's anything that's too controversial and ahead of its time for Bitcoin, Litecoin can try it first and report the results. Certainly, this role is valuable and brings many benefits to the space. And to all the pioneers who stick around and support this mission: I salute you!




BITCOIN
TAKEOVER
PODCAST
SEASON 15
HODLING
SIDESHIFT.AI
STARKWARE
BTCTKVR

HOW LITECOIN HELPS BITCOIN?



LITECOIN LITECOIN LITECOIN LITECOIN LITECOIN LITECOI

At first glance, it might appear that Bitcoin and Litecoin find themselves in a state of competition: they have a nearly-identical open source software architecture, they aim to accomplish the same goal of enabling digital payments around the world in a decentralized way and without a trusted third party, and they offer different currencies from which users can choose.

As a matter of fact, there are some folks from amongst the Bitcoin maximalist group who refer to Litecoin as "inflation" to the 21 million hard cap: since Litecoin is so similar with Bitcoin and inherits the same codebase, it adds another 84 million coins to the market. Some critics also take this argument further in order to imply that Litecoin's existence diminishes the desire for users to pay Bitcoin's higher main chain fees.

But nobody who understands the spirit of free open source software and also knows how markets work would make such an assessment. Firstly, because a fork of the codebase makes more developers work on it — and therefore provides extra testing, research, and development to the original implementation. Secondly, because there's definitely a market for inexpensive and fast transactions on a decentralized and immutable ledger that's secured by Proof of Work. As Bitcoin fees rise and the user experience for second layers remains too cumbersome for the average person, the free market will search for alternatives with little to no consideration for any ideology: it's only a matter of finding the best tool for the job.



Now let's take a walk down memory lane to present the moments when Litecoin has been instrumental in helping Bitcoin improve. It all starts with the Genesis Block, which Charlie Lee mined on October 13th 2011. At the time, it didn't seem evident... but five years later, the Litecoin creator would demonstrate how Satoshi Nakamoto should prove that he is the creator of Bitcoin. He signed the Genesis Block using his private key, by typing the message "I, Charlie Lee, am the creator of Litecoin". The cryptographic proofs were valid, so no further claims or stories were necessary. Why is this such a big deal? While some bitcoiners were genuinely getting fooled by Craig Wright's stories, Charlie proved how it should be done in practice — and this couldn't be possible in the absence of a fork with a similar design, whose creator is still actively involved.

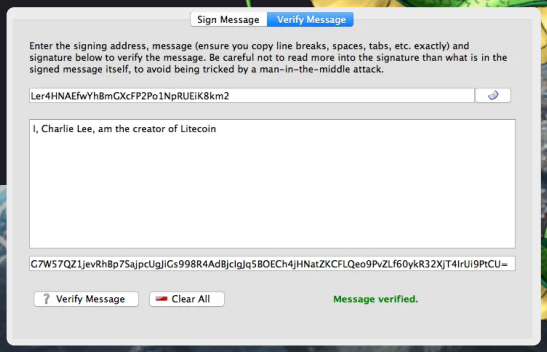
In 2017, at the peak of Bitcoin's scaling debate when the SegWit soft fork was regarded with skepticism, Litecoin embraced this upgrade. Charlie Lee took the time to speak with the miners in order to reach consensus, so that the new Bitcoin improvement would be proven safe to the rest of the world. SegWit, which fixes a malleability bug, enables the Lightning network, and also introduces a creative way of increasing



the block size. However, it was never a necessity for Litecoin — the fees were weren't high and the blocks rarely ever filled to full capacity. But it was a calculated risk in order to legitimize Litecoin as Bitcoin's little brother, the one who can make bold moves with experimentation and minimize the costs of potential errors.

The SegWit story was a real success — a fact that the free market echoed

CBDCS & SURVEILLANCE CAPITALISM



and reflected on the price of LTC. This incentivized testnet approach proved to be a brilliant idea. So Litecoin amped it up to 11 with the Lightning Network. Back in 2018, doing Lightning stuff outside of the safe environment of testnets was often described as "reckless". Many bitcoiners were skeptical about this layer two, while developers were reluctant to lose BTC with their experimentation. This is why much of the early testing took place on Litecoin. Companies such as ACINQ and Lightning Labs quickly became interested in using Bitcoin's favorite ally for their layer two projects. After all, they could just copy the successful code and paste it on top of Bitcoin with little to no adjustments. Given the conservativeness of Bitcoin, the Lightning network couldn't become such a rapid success without involving Litecoin.

There's also something to be said about merged mining with Dogecoin. Though the culture of monetary maximalism in Bitcoin effectively prevents such an implementation from happening (and some analysts suggest that merged mining contributes to centralization), it's provably good for increasing the miners' revenue. The idea of Merged Mining was first proposed by Satoshi Nakamoto himself, when Namecoin (a separate blockchain network for data and domains, which was launched as the world's first altcoin) became popular. Essentially, merged mining is about using the same Proof of Work to secure two different networks, thus also enabling miners to collect rewards in all currencies involved.

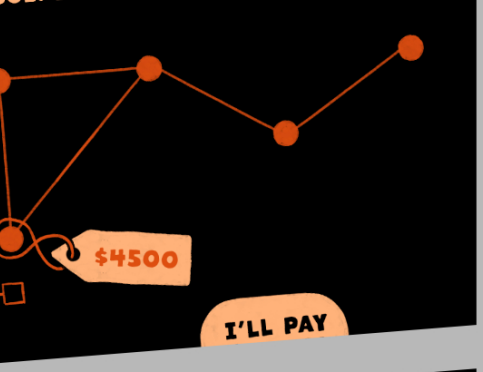
Since August 2014, Litecoin has taken Dogecoin by the paw to feed it with the world's largest portion of Scrypt Proof of Work miners. But what started as an act of benevolence for the sake of preserving a meme and its community has grown into a beautiful friendship which provides mutual support: as LTC miners see their rewards getting halved every four years and the price doesn't always go up, there is still a profit to be made from DOGE rewards. Since Elon Musk turned the cute dog money into the unofficial currency of his ventures (with Tesla even accepting dogecoins in their merchandise store), the coin depicting the world's most popular Shiba Inu has truly started a space exploration of its own. Today, it's not unusual for Dogecoin to register higher daily transaction volumes than Litecoin — but it's the Litecoin network that provides the security infrastructure.

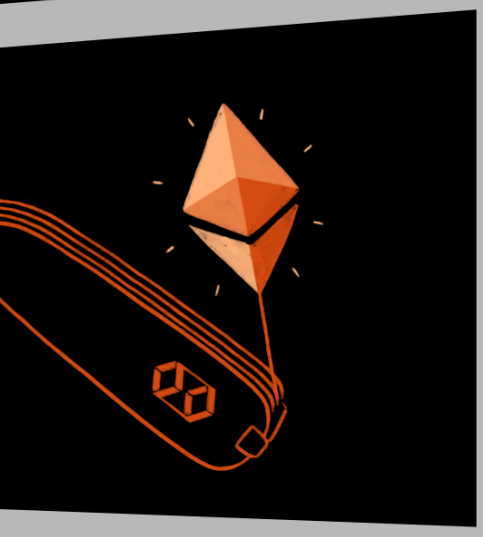
This symbiosis can inspire bitcoiners to also consider securing other SHA256 coins. Sure, most community members probably hope that BCH and BSV will fail, as a symbol of having won the scaling wars. But Bitcoin should also have a sidechain with big blocks, which enables anyone to get onboarded with low fees while holding their own keys, whose validation and storage is optional among node operators, and that gets merge mined with BTC. The currency doesn't have to be entirely different — it can even be BB-BTC (Big Block Bitcoin), a layer two token that's backed 1:1 by BTC locked on the base layer.

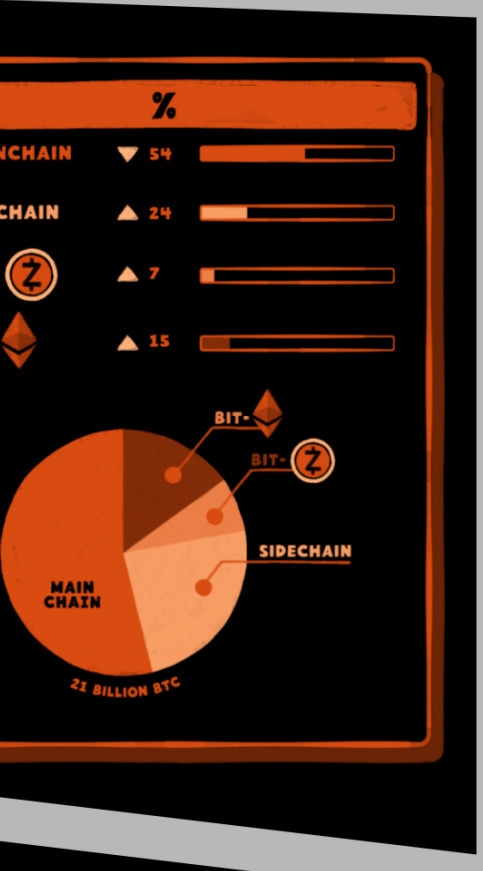
There's already a proposal for this which was initiated by Paul Sztorc, whose idea of Drivechains (as described by BIP300) is becoming increasingly popular over the years… and once again, Litecoin appears to be more open to the idea. As Charlie Lee revealed in S15 E34 of the Bitcoin Takeover podcast, once all the fine details surrounding MWEB (MimbleWimble Extension Block) get finalized and there is enough support from various types of wallets, Drivechains might be the next big improvement.

Speaking of MWEB, it's currently the best privacy and scaling proposal that's 100% compatible with Bitcoin, has a battle-tested implementation that's been around for a couple of years, and can be activated through a soft fork. All previous ideas, from Confidential Transactions to ring signatures and ZK SNARKs, require hard forks and much more radical changes to the overall design. Not Litecoin's MWEB, though: Bitcoin can activate it just like it did with SegWit and devs can build apps on top of it just like they ported Lightning network clients from one network to the other.

Given all the useful research and development that it creates, Litecoin is a net positive for Bitcoin — and possibly its greatest ally, as it puts skin in the game whenever a significant improvement proposal rises to prominence and then provides incentives for anyone who's capable of improving the design. Haters gonna hate, but the Chickun will keep on arising and helping Bitcoin.

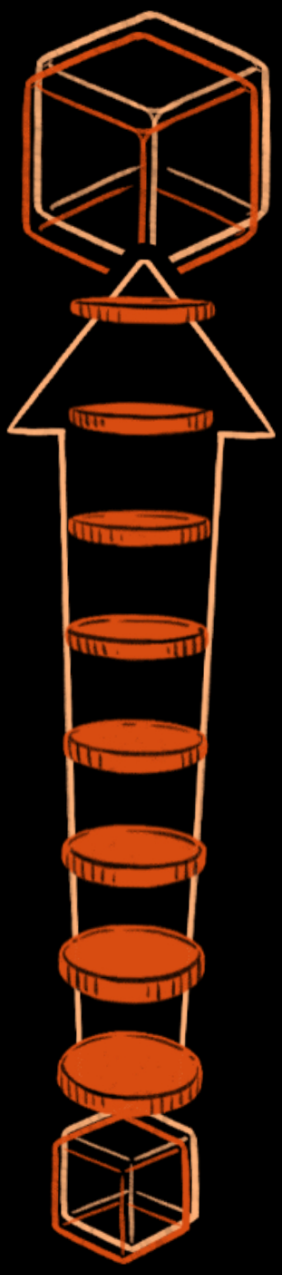






MULTIPLE BLOCKCHAINS

LAYER 2



84 LAYER 1
~~21~~ MILLION
~~BTC~~ LTC

EASILY SWITCH NETW





LayerTwoLabs.com

ain all altcoins of their use cases &
onboard 8 billion people
today!

BITCOIN VS LITECOIN

What are the differences?

When Bitcoin maximalists talk about Litecoin, they often refer to it as a lazy fork: the same codebase, with 4 times faster block times and 4 times the supply. They'll call it the result of a copy-paste operation, with no technological merit or legitimacy. However, there's more to the picture than meets the eye.

Yes, Litecoin has a supply cap of 84 million coins (as opposed to Bitcoin's 21 million). Of course, a new block gets mined every ~2.5 minutes (instead of Bitcoin's 10) and the mining difficulty adjustment happens every 3 and a half days/504 blocks (as opposed to Bitcoin's 14 days/2016 blocks). The reward halving also happens every 840.000 blocks... but due to the faster block time, the interval between epochs is still that of 4 years.

Naturally, the marketing narratives are different: Bitcoin is digital gold, while Litecoin is the silver equivalent. And yes, the messages in the genesis blocks are different too: Satoshi Nakamoto famously immortalized a political statement ("The Times 03/Jan/2009 Chancellor on brink of second bailout for banks"), while then-Google engineer Charlie Lee referred to the most discussed piece of news in the world of technology ("NY Times 05/Oct/2011 Steve Jobs, Apple's Visionary, Dies at 56").

But these facts merely scratch the surface. Many of the early Bitcoin clones feature similar changes of parameters — but why did Litecoin survive for almost 13 years while every other early altcoin is dead? Well, the most significant answer can be found in the mining algorithm. Compared to Bitcoin's SHA256, Litecoin's Scrypt is more memory-intensive. In the early days, this was essential for encouraging GPU miners (who were no longer profitable due to the emergence of Bitcoin FPGAs and ASICs) to switch to mining LTC.

It was Scrypt that built communities in 2011-2013 and determined Bitcoin OGs to repurpose their stacks of graphic cards. And it was also Scrypt that kept the Litecoin network secure from 51% attacks that might have come from Bitcoin ASICs — in other words, this radically different mining algorithm played an essential role in bootstrapping the first adopters and then in establishing LTC as the prime altcoin.

Since the summer of 2014, Litecoin also adopted Dogecoin via merged mining. After all, the enthusiastic community of Shiba Inu lovers was just too nice to face the brutal reality of 51% attacks. In the beginning, it was a mere act of sympathy and benevolence from Charlie Lee. But since Elon Musk started tweeting about the cute dog money, DOGE became an essential part of every Litecoin miner's revenue. Ironically, the security budget concerns were fixed by a good boy.

Sure, Bitcoin was the first to have merged mining with Namecoin, the original altcoin. But this relationship didn't last, as the main use case (registering domains in a decentralized way) never took off and the demand for NMC faded into obscurity as miners dropped their support and many users embraced monetary maximalism. Today, the only merged mining that Bitcoin has is through the Rootstock (RSK) sidechain — with 50% of the hash rate being involved in securing this network. However, Rootstock doesn't have a different base currency: it uses



BTC that's locked on the base layer and issued on the parallel chain, so the miners only earn extra revenue from transaction fees. It's also unlikely that the Bitcoin community would agree to save the other SHA256 coins (BCH, BSV, DigiByte) through merged mining. So there won't be any extra revenue coming from altcoins, like in the case of Litecoin and Dogecoin.

Speaking of merged mining and two-way pegs, there's a certain proposal that's called Drivechains. It was introduced as BIP300 on Bitcoin, but it faces pretty strong opposition from some of the more conservative-minded developers. Through it, Bitcoin would be able to have a sidechain for pretty much every interesting use case (smart contracts, privacy, prediction markets, big blocks). Interestingly, during S15 E34 of the Bitcoin Takeover podcast, Charlie Lee hinted that Drivechains might be coming to Litecoin after the work with MWEB is completed. So once again, Litecoin finds itself at the forefront of Bitcoin-compatible experimentation.

This trend of openness to innovation is something which provides extra value to the network: it's a testnet with good enough incentives, that developers who can't prove the worthiness of their work in the more conservative Bitcoin space can use. Back in 2017, there was a lot of FUD surrounding SegWit — so Litecoin obliterated it in practice (as opposed to publishing long Reddit posts and sending compelling e-mails to the bitcoin-dev mailing list). When the Lightning network was thought to be reckless, it was the early developments on Litecoin that showed that it's safe enough for the Bitcoin mainnet. And when the common belief was that privacy and scalability can only get added through a hard fork, Litecoin embraced MWEB: the MimbleWimble Extension block, a beautiful marriage between two of the most interesting technologies in the space.

Today, Litecoin regularly updates to keep up with the two of the most cypherpunk and decentralized codebases in the space: Bitcoin Core and Grin++. The community dared to embrace this approach to privacy as a way to acquire monetary fungibility — and the entire industry is now paying attention to the development of MWEB. Sooner or later, the Bitcoin community will also have a serious debate about soft forking a privacy upgrade. This is when Litecoin will once again prove itself useful for undergoing incentivized testing of avant-garde features for multiple years.

There's also something to be said about philosophical differences: Bitcoin pursues a path which makes it a digital commodity much more than a currency for everyday spending. On the other hand, Litecoin is laser focused on commerce and merchant adoption. The metric for Bitcoin's success is the price increase. In Litecoin's case, it's transaction volume and ranking in popular marketplaces or payments processors.

In order to support the idea of financial sovereignty, Bitcoin added RBF (Replace By Fee) to enable users to increase transaction fees or else cancel transactions (broadcast a transaction with a higher fee, whose recipient is the same sender). No Bitcoin transaction is final until at least one block confirmation has happened. Litecoin, on the other hand, embraced the zero-confirmation path: transactions are declared final the moment they get broadcast under a "first seen" rule, so there's no way to make any changes once the nodes have picked up information about the transaction. Bitcoin is optimized for high-value transactions for which the receiver can wait for 10 minutes or longer. Litecoin can be used to make quick purchases, under the guarantee that every transaction that gets broadcast is irreversible even before it's mined.

Though Bitcoin and Litecoin share a common codebase and have multiple similarities in terms of functionality and end goal, they differ in both technical specifications and philosophy. At this point of its existence, the digital silver coin has acquired its own identity and comes with a distinct value proposition. Those who get it, are very much ahead of their time. All the others are either stuck in the world of monetary maximalism, or else they chase fleeting trends. In the end, truth shall prevail and the best money tech will win.



LITE.SPACE

CROWDFUNDING LITECOIN PROJECTS, ONE OPEN-SOURCE PROJECT AT A TIME.





LITECOIN CORE



LITECOIN SPACE



ORDINALS LITE



MWEB



LITECOIN DEV KIT



LITESCRIBE



LITEWALLET



ELECTRUM-LTC



MWEB + BTCPAY

WHY IS LITECOIN SO USED IN COMMERCE?

If you look at reports from payment processors such as BitPay and merchants such as Bitrefill, you're going to notice that Litecoin constantly ranks among the top 3 payment options. In hindsight, the reasons are simple: the transaction fees are negligible, the confirmation time is fast, and there is no way for the user to double spend the transaction through RBF.

However, there are dozens of other coins which fulfill these technical criteria: from Dash to Dogecoin, you're going to find plenty of contenders. Heck, nowadays you even have stablecions on low-fee networks such as Solana and Tron. So what makes Litecoin so special?

First of all, brand awareness and network effects are extremely important. Litecoin has been around since the fall of 2011, has grown organically over time, and managed to survive every subsequent bear market. Many people know about it, and the "digital silver" narrative has also helped in defining the purpose of this money system.

Secondly, Litecoin's technical similarity with Bitcoin makes it easy to integrate everywhere BTC is also accepted. Spinning up a full node to process transactions takes only a few hours, and ATM or PoS firmwares don't require any special adjustments or complex software updates in order to add LTC as a payment option. There's also something to be said about the identical user experience that you get with Bitcoin and Litecoin: users don't need to learn anything new, they use the same features and interfaces with which they are already familiar. Simplicity and convenience matter, so the projects which offer them are destined to reap all the benefits.

Thirdly, there is a community of enthusiastic users who constantly increase the demand for Litecoin by using the "pay & replace" strategy. A supply of technical specifications is worthless in the absence of usefulness to humans — and the LTC community consists of people who work to spread adoption across all market cycles. While BTC had a much better market performance, with the price increasing significantly after every reward halving, Litecoin has been a much more rough asset for long-term HODLers. But the fact that there are people who use it for payments even if they aren't always benefiting from an increased purchasing power (or they don't outperform stock market







indexes) proves that there's more to the picture than meets the eye. Litecoin is fast, affordable, censorship resistant, and permissionless. So the value proposition is not to hoard large amounts of coins and hold them speculatively, but to participate in commerce. Many users most likely swap other coins for LTC, then send payments to shops, exchanges, P2P counterparties, and processing companies.

Critics will point out a technical flaw in this model: that Litecoin would have high fees and confirmations that take hours just like Bitcoin if the number of users was equal and the market price increased proportionally. And no, the faster block times don't really provide guarantees of quick confirmations in a high-fee environment.

But Litecoin's culture and philosophy would push the network to scale towards preserving the low fees and fast confirmations. It makes no sense for the project to follow Bitcoin's "digital gold" and "store of value" approach. Litecoin must retain its competitive advantage and, before being a specific technical implementation, it's an idea and an aspiration to achieve certain monetary goals.

There's also something to be said about MWEB as a scaling layer: it doesn't only increase privacy, but also future-proofs the network with a throughput boost. So if Litecoin gets the same amount of users and transactions, they won't pay the exact same transaction fees —they will be at least 50% lower.

But how is this sustainable in the long run, as miners collect fewer fees after every halving cycle and the price doesn't necessarily double every 4 years? Well, the answer is that the miners will collect more fees from more transactions taking place across multiple blockchains. Today, Dogecoin is merge mined with Litecoin: therefore, LTC miners also collect fees in DOGE and participate in the issuance of new coins. In the future, the potential activation of Drivechains might significantly increase the number of users and allow fee collection across smart contract, privacy, and prediction market sidechains. This way, the fees can always stay low while an increasingly high number of users engage in various types of economic activities.

Litecoin doesn't aim to compete with Bitcoin directly, but completes it and provides useful feature testing. It benefits from innovation much sooner thanks to a culture that's much friendlier with change, but also remains similar enough with Bitcoin to enable easy application porting and user migration. Long term, it can also be regarded as a source of market pressure for Bitcoin to improve: if the digital gold seeks to become a more efficient medium exchange, it must learn some lessons from Litecoin and borrow some of the well-tested tech.

But for as long as BTC users prefer to HODL speculatively instead of spending, there will be a demand for alternatives which work similarly but provide extra desirable features. This is why Litecoin is the king of payment coins and will most likely remain so for years to come.



#LITECOINFAM

MEMBERS WHO DONATED 1 LTC TO THIS MAGAZINE



@I_MAKE_LEMONADE

@FR333DOOOM

@ANML_LITECOIN

ALAN AUSTIN

@84MILLION

CHARLIE G

@LTCCOFFEECLUB

ROLAND HRUBARU

@LTCUNDERGROUND

GALAL DOSS

@NAKAMOTO_STD

PATRICK B. DUGAN

@HOLANGLITTE

BTSTATTOOS.COM

@BENMIKLOZEK

LUKAS JAKOB



🤑 **Donate**

✍️ **Write your name**



THE BEST LITECOIN WALLETS

"every monetary unit exists on a blockchain"

When referring to cryptocurrencies, the term "wallet" is slightly misleading: in real world, the wallet is an accessory which holds your money. But in the case of Bitcoin and Litecoin, the wallet is merely a private key management software which allows you to sign and broadcast transactions to the network. The coins aren't held in these wallets per se — every monetary unit exists on a blockchain, but only the correct private key can spend its corresponding amount. So if you lose the device on which this wallet is stored or you accidentally delete the software, it's not the end of the world: you can always recover your funds if you have the private key stored somewhere safe. But even if you do lose access to your coins and they are forever lost, the network doesn't know what happened: it assumes you're just long-term HODLing, and keeps the units as part of the monetary supply forever.

Yet for convenience, in spite of the semantic differences, we still refer to these key signers as wallets. From the get-go, we must make it clear that not all wallets are created equal and you must know the differences. Also, I should mention that this article only recommends the best solutions for Litecoin users.

First and foremost, there are full node wallets (**Litecoin Core**) and lightweight wallets (Litewallet, CakeWallet, Ballet, Guarda, Exodus, Coinomi, Electrum without a full node). This distinction is important in the context of running sovereign free open source software: if you're serious about using Litecoin, you should run only Litecoin Core on your computer and something else that points to it on your mobile. This argument alone narrows down your portability option to Litewallet and BitBoxApp — as only these two give you the option to connect your own full node. If you want to swap your LTC for Monero or buy gift cards for popular stores and services, Cake Wallet is also excellent (but is more of a complimentary tool which shouldn't replace the mightier wallets that connect to your full node).

Secondly, if you're going to store large amounts of LTC for a long time, then it's definitely a good idea to get a hardware wallet or a cold storage device. What's the difference, you say? Well, hardware wallets are a middle ground between the security of cold storage devices (Casascius Coins, BTCC Mint, Ballet, paper wallets) and the convenience of hot wallets (most famously, Electrum in SPV mode). Now that we established that hardware wallets are a useful hybrid, it's time to recommend the best of them: Trezor (any model is fine), BitBox02, and KeyStone.

Trezor is uncompromisingly open source and has a record of offering support for their devices since 2014. The team behind Trezor created BIP39 (which allows you to convert the non-readable private key to a more friendly string of 12/24 words) and BIP44 (which allows you to store multiple coins such as BTC and LTC under the same seed phrase). Today, both of these are industry standards... and it's no wonder that most hardware wallets on the market are rebranded Trezor forks.

The main drawback is that only two of the three Trezors models available on the market in 2024 have a secure element chip to offer physical protection against private key extraction — but the team is reluctant to use closed-source chips that you can't verify and which also require the company to sign NDAs to not publish potential bugs. The most popular device, which has been available on the market since 2014, has sold millions of units, and everyone probably already has one in a drawer, doesn't have such a chip. Trezor's philosophy since day one has been that of focusing on software development, and then optimizing it around the existing





hardware. So there's an ongoing process of improving the product through security patches that result from user feedback — if someone is able to find a vulnerability, there's a bounty that can be collected in exchange for disclosing the issue.

A research division from Trezor is also working on the Tropic Square project, which is expected to release the world's first open source secure element chip sometime in 2025. Until then, the suggested solution to gain physical security is to create a passphrase for your wallet (which is generally great, unless you lose it or forget it). If you want to buy a Trezor hardware wallet and support the BTCTKVR magazine project, you can use the affiliate links in the table at the end of this article.

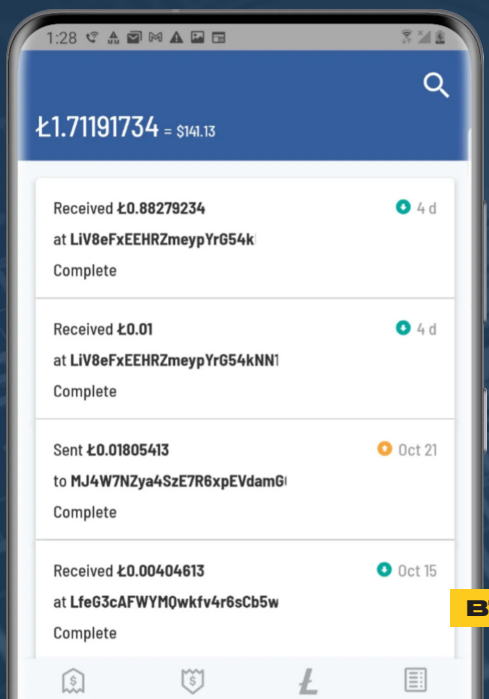
On the other hand, the **BitBox02** is a different beast: built from the ground-up by the technical ambitions of Bitcoin Core developer Jonas Schnelli, this Swiss-made machine was designed with desktop and mobile connectivity in mind. This is why it comes with a USB-C male connector that you can insert in your computer or in your Android phone. For physical security, the BitBox02 features the ATEC608B chip — a general-purpose security chip that you can also find in BTC-only wallets such as Coldcard and Foundation Devices Passport. However, the guys who built the BitBox are fully aware of the tradeoffs involved and have programmed the firmware to isolate the chip and only use it for its most basic purpose. The BitBoxApp user interface also enables you to connect your own full node (Litecoin Core with Electrum server indexing), so you don't have to trust in the company's servers. Interestingly, this feature also works on Android wallets — thus making the BitBox02 the second best mobile wallet for Litecoin, with better security but fewer features (most notably, no MWEB support).

Just like in the case of Trezor's Suite, the BitBox02 companion app also offers the option to connect to their server via Tor — this network-level obfuscation will make the company unable to know where you're based while using the device. It's a neat workaround for the people who want some privacy, but are unable to connect their own full node.

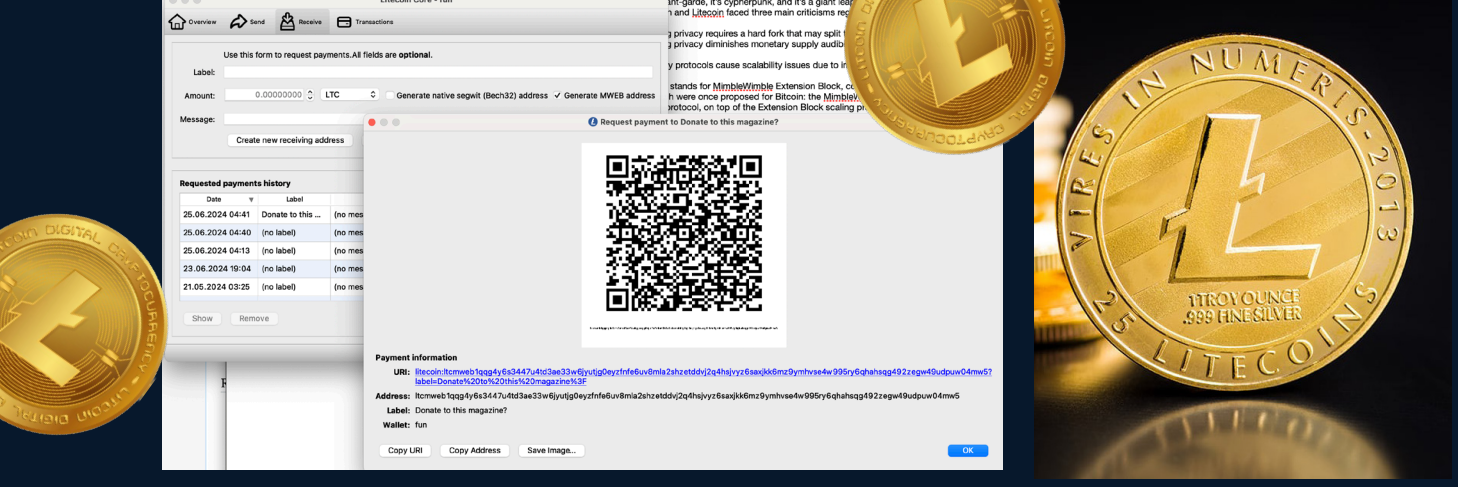
Something unique about this Swiss-made hardware wallet is the "anti-klepto" system, which verifies the integrity of the firmware to prevent nonce covert channel attacks. And if you're too lazy to write down your 12/24 words on a piece of paper (which you shouldn't be), you get the option to do a quick backup & recovery through a micro SD card that comes included in the box. It's definitely convenient, but keep in mind that SD cards aren't optimized for long term data storage — if you don't connect them to your computer regularly to check the integrity of the data, they can become corrupted due to physical or environmental reasons.

The BitBox02 is tiny, well-built, features touch sensors for input, and is made in Switzerland. If you're going to buy a one, you can also support the BTCTKVR magazine project by using promo code BTCTKVR at checkout — you should get a 5% discount too!

Last but not least, the **KeyStone** is the Chinese underdog which delivers lots of features at a pretty good price. On the open source spectrum, it's not as transparent as the Trezor and BitBox hardware — a criterion that matters in the context of minimizing trust in the manufacturer. But on the feature and user experience spectrum, it's the most generous: it comes with a camera to scan QR codes,







it includes a sufficiently-large 4-inch touch screen, and it's marketed as being completely airgapped (you can use the device without ever connecting it to the internet and without plugging it into a computer that's connected to the internet). In regards to the airgap, though: you do need to be connected to the internet to check the latest state of your coin balance and to broadcast transactions to network nodes. So the way in which the airgapped mode works is that you sign transactions from your KeyStone, and then copy the resulting file to an external media storage device (SD card) that you finally plug to your computer for the broadcasting part (an operation that's possible with PSBT-compatible wallets such as Electrum). Of course, this is optional — you can still use the device with a USB connection to your computer. What's interesting about the KeyStone is that it includes a fingerprint scanner and a user experience which very much resembles that of a smartphone — so the learning curve is very smooth.

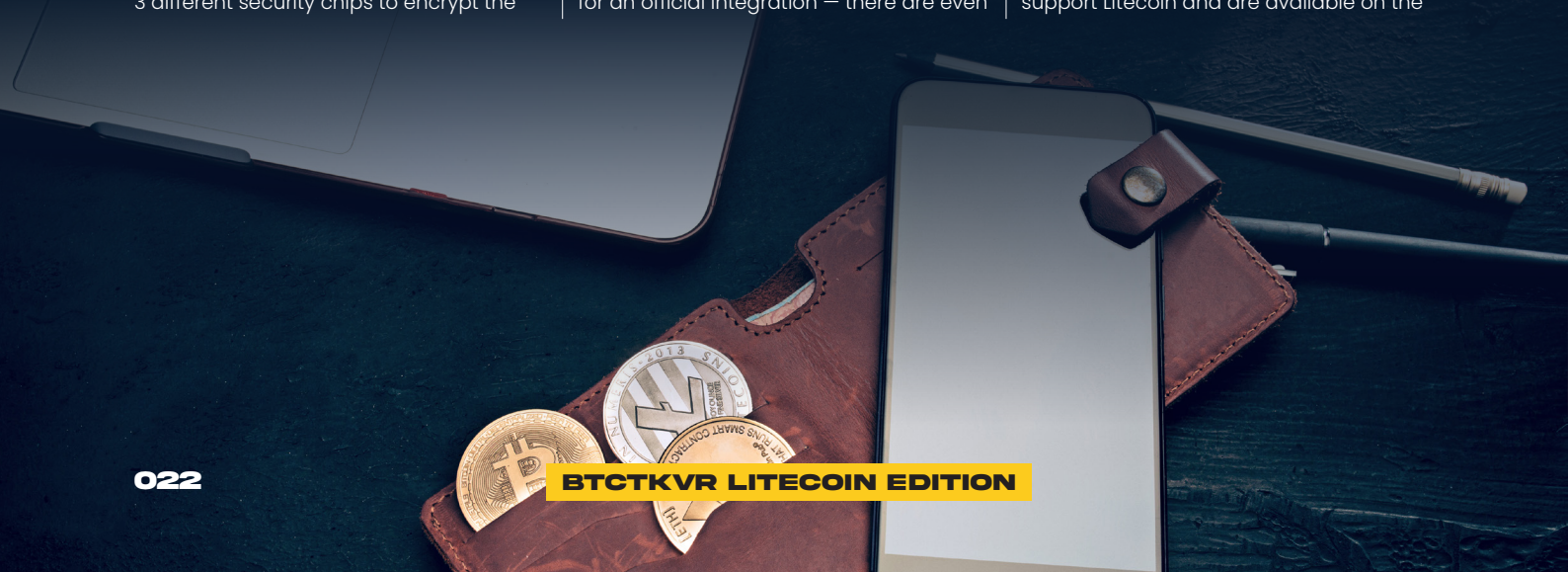
Other features include entropy via dice rolls (do at least 100 if you want to get better randomness than the electronic Random Number Generator), the simultaneous storage of 3 seed phrases, a rechargeable battery, and easy access to advanced functions such as multisig and Shamir Backup (SLIP39, also available in Trezor Safe 3 & 5). It also comes with 3 different security chips to encrypt the user's fingerprint and seed phrases. But all of these benefits come at the expense of a lower degree of auditability and open sourceness: if the Trezor is simple, the subject of hundreds of clones, and much more battle-tested, then the KeyStone is very complex and much more difficult to verify due to the presence of the closed-sourced security chips. If you want to buy a KeyStone for your Litecoin holdings, type this link and support the BTCTKVR Magazine project: https://bit.ly/3x1ngHA

Interestingly, none of the hardware wallets on the market support Litecoin's MWEB... at least, not yet. But after Litewallet makes it possible to run the extra features on a lightweight client, it's only a matter of time until these companies pick up the free open source code and integrate it. If there is enough community demand, the companies will definitely start supporting MWEB for Litecoin.

As you might notice, some big names like Ledger and KeepKey are missing. The reason is simple: the former has made some questionable decisions in terms of enabling their users to self-custody, while the latter is no longer being maintained. Interestingly, Litecoin contributor Hector Chu did create a way to use MWEB addresses on a Ledger Nano S, through a custom firmware which leverages the power of Electrum wallet. However, the user experience is not necessarily optimal and it's probably better to wait for an official integration — there are even rumors that Trezor would collaborate with any dev who wants to bring MWEB to their Suite app. And if Trezor does it, then it's easy for other manufacturers to copy the feature. Even if it's popular and lots of people already own Ledger devices, it's hard for me to recommend them.

There are also dozens of other devices that make dubious claims or offer nothing interesting for Litecoin users. Many of them are not really open source and require a higher degree of trust. Devices such as CoolWallet, Tangem, SecuX, Keevo, SafePal, and ElliPal cost pretty much the same as the solutions recommended in this article, but offer fewer options for Litecoin users. Overpriced hardware wallets such as nGrave make big claims, but don't offer all the software options that you can find in the KeyStone. Remember: a hardware device without proper software to back it up is just a fancy piece of plastic and/or metal. And once again, Trezor is the only one that's been battle-tested and refined for longer than a decade, while BitBox02 is the only one that lets you connect your full Litecoin node and is fully optimized for both computers and Android phones. If you want to scan QR codes and generate your own entropy via dice rolls, you can only do that on the KeyStone. There are no ideal models, only tradeoffs.

There's also something to be said about cold storage devices which support Litecoin and are available on the





market in 2024. **Ballet** is definitely known within the community, as the project was created by Charlie Lee's brother — and the company behind the wallet regularly sponsors the annual Litecoin Summit. Inspired by Casascius and BTCC Mint, these metal cards have a premium feel and benefit from the extra convenience of a mobile app. Ballet appeals to two different audiences: non-technical people who don't mind reusing the same address to store their coins for the long term, as well as collectors who enjoy buying pre-loaded editions (such as 2023's Litecoin Block cards, which include 6.25 LTC on a 50-gram fine silver card).

Bobby Lee takes pride in the simplicity of his solution and, as he revealed in S5 E1 of the Bitcoin Takeover Podcast, he even gifted some loaded Ballet cards to Bruce Willis and his daughters. But the main issue with Ballet is the implied trust in the manufacturer: since the Pro series was discontinued, users can no longer generate their own BIP38 private keys. So Ballet undergoes this rigorous process of printing the private keys on the cards in different parts of the world, with the CEO of the company vouching with his reputation that there will never be any theft of funds. For some people, this is good enough — but others might want more advanced solutions which mitigate the trusted setup and don't make it obvious how many coins every user owns (Ballet even publishes on their home page the total valuation of their users' coins, which some privacy-minded people may not like).

For more advanced users who don't like the idea of a trusted setup and want to enjoy the benefit of a cold storage card with some extra features (NFC tapping, card reader that works with your computer, compatibility with Electrum wallet), there's Satochip. Powered by Java cards, these devices cost approximately $25 and work either with the companion app or with Electrum Litecoin via USB card reader.

Satochip also produces two other types of cards: the Satodime, which is designed to act like a bearer asset (basically a paper wallet with a sealing mechanism that needs to be tampered in order to withdraw the coins), and Seedkeeper (a storage solution for your passwords, private keys, and seed phrases). Everything about these Java cards and their software is open source and auditable — with the exception of the EAL6 certified chip, which operates like a black box for the input data. To learn more about Satochip, listen to S15 E20 of the Bitcoin Takeover podcast — where creators Bastien and Baudoin explain how the device works and also perform a live demo. And if you made up your mind about giving Satochip a try, use promo code BTCTKVR at checkout for a 5% discount.

Last but not least, you have the custodial exchange wallets. All I'm going to say about them is: stay away and only use for small amounts if you're trading! It might seem convenient to custody your coins with a business that has a good reputation in the field, but the risks outweigh any benefit. Today, the user experience for freedom wallets is really easy, as storing 12/24 words on a piece of paper (or on a metal backup such as **Cryptosteel**) has been greatly simplified. There's an entire industry that makes self-custody accessible for everyone and it feels much better to watch the collapse of the next FTX from the sidelines, knowing that your coins are not affected. It's also a matter of freedom: while some exchanges and custodians might limit your withdrawals or restrict to whom you can send transactions, your own wallet lets you send money to anyone around the world without asking for permission. As Satoshi (and his disciple SatoshiLite) intended!

So no matter which wallet you choose, make sure it's the one that suits your needs: if you need privacy and want to verify your own transactions, make compromises and go for the full node. If you spend the coins frequently, then mobile wallets such as Litewallet and BitBox02 are excellent. If you want to HODL for the long term, consider a hardware wallet like Trezor, BitBox02, or KeyStone... or else choose a cold storage device such as Ballet or Satochip. And if you're a trader, make sure you withdraw from exchanges frequently — don't use these exchanges as banks!



WALLET	TYPE	CONNECTS TO YOUR OWN LITECOIN FULL NODE	MWEB SUPPORT	PROS/CONS	PRICE
Litecoin Core	Desktop	It is the full node	✅	✅ the OG wallet that will always include the new features; ✅ best privacy & sovereignty; ⛔ only works on a desktop/laptop, requires a full day sync & ~100 GB in local storage.	Free
Electrum Litecoin	Desktop	✅	✅	✅ lightweight, connects to a random full node but also works with your own; ✅ enables full node access to Litewallet, BitBox02 & more; ⛔ not updated/maintained regularly for Litecoin, not the most user-friendly wallet.	Free
Lite Wallet	Mobile	✅	✅ Q4 '24	✅ LTC-only, built by OG Litecoin devs; ✅ updated regularly, is the first mobile wallet to include the latest features; ⛔ transaction fees are higher due to a dev tax.	Free
Cake Wallet	Desktop/ Mobile	❌	✅ Q4 '24	✅ the best multi-coin wallet for Litecoin, allows you to swap LTC for Monero, Bitcoin, Ethereum & Tether; ✅ use your LTC to buy prepaid cards & gift cards via Cake Pay integration; ⛔ doesn't let you connect your own Litecoin full node.	Free
Trezor One	Hardware	❌	❌	✅ the OG hardware wallet, battle-tested since 2014; ✅ easy user interface, large enough screen to verify transactions, physical buttons; ⛔ doesn't support advanced Litecoin features, no secure chip. 🍀 use this link to support the **BTCTKVR Magazine**: https://affil.trezor.io/SHXt.	$64
Trezor Safe 5	Hardware	❌	❌	✅ easier to use than Trezor One, with a larger screen; ✅ you can type your passphrase directly from the device; ⛔ doesn't support advanced Litecoin features. 🍀 use this link to support the **BTCTKVR Magazine**: https://affil.trezor.io/SHXs.	$180

WALLET	TYPE	CONNECTS TO YOUR OWN LITECOIN FULL NODE	MWEB SUPPORT	PROS/CONS	PRICE
Trezor Safe 3	Hardware	❌	❌	✅ the middle ground between the Trezor One and Safe 5, at a very affordable price; ✅ includes a security chip whose code is open source; ⛔ doesn't support advanced Litecoin features; 🍀 use this link to support the **BTCTKVR Magazine**: https://affil.trezor.io/SHXr.	$85
BitBox02	Hardware	✅	❌	✅ works with both computers and Android; ✅ lets you connect your own Litecoin full node; ✅ includes a security chip and lots of cool ; ⛔ the input sensors for typing aren't always very accurate; 🚀 5% discount with promo code **BTCTKVR**	$161
KeyStone 3 Pro	Harware	❌	❌	✅ looks and feels like a smartphone, very easy to use; ✅ basically what CoolWallet, Tangem, SecuX, Keevo, SafePal, ElliPal & nGrave are trying to be; ⛔ on the open source spectrum, it's the least transparent device from this review; 🍀 use this link to support the **BTCTKVR Magazine**: https://bit.ly/3x1ngHA.	$141
Ballet Real Litecoin	Cold Storage	❌	❌	✅ newbie-friendly, very good for onboarding boomers; ✅ well-built, sturdy, comes with a convenient smartphone app; ⛔ lacks support for advanced Litecoin features; ⛔ relies on a trusted setup, for which Ballet generates the private keys before delivery.	$39
Satochip	Cold Storage	❌	❌	✅ uses smart card technology for secure cold storage; ✅ NFC-compatible, you can tap it to your phone to check balance; ✅ great for physical collectibles and everyday use ⛔ lacks support for advanced Litecoin features. 🚀 5% discount with promo code **BTCTKVR**	$25
Cryptosteel	Metal Backup	❌	❌	✅ metal backup for your passwords, seed phrases, passphrases, private keys, and everything else you want to protect; ✅ blockchain-agnostic, resistant to earthquakes, floods, fires & all sorts of hazards; ⛔ more expensive than its Chinese-made clones on the market. 🚀 10% discount with promo code **BTCTKVR**	$96



INTERVIEW WITH PAUL SZTORC

CEO of LayerTwo Labs, Creator of Drivechains & Keynote Speaker at the 2024 Litecoin Summit

Vlad: *How would you describe Drivechains to a non-technical Litecoin user?*

Paul: Send your LTC to *different software* and back.

For example, send to an EVM compatible blockchain, to do Ethereum-style contracts. Or, send them to a zk-snark blockchain, to access z-addresses and more privacy. There will only ever be 84 million circulating LTC, across all the chains.

Each drivechain grants scale-throughput, AND new fee revenues to Litecoin miners.

Vlad: *What type of majority do Drivechains require from miners and/or from validating nodes in order to activate?*

Paul: In theory, 51% hashrate alone is sufficient.

In practice, hashrate fluctuates — so ideally, the precise target should be closer to 70%. Once achieved, this majority will orphan any offending blocks, fully activating the feature. This does have the "impolite" effect of 70% strong-arming the remaining 30%. (Whether this is a bug or a feature, is up to you!)

Ideally, a few big whales and big LTC services would also upgrade — this would discourage miners from ever co-ordinating to de-activate (unless there was some reason to do so).

Vlad: *What are some of the most notable features that Drivechains can bring?*

Paul: Drivechain allows everyone to use LTC however they like, with minimal in-fighting. If you are serious about getting to 8 billion users, then this is going to be necessary. Different people want different things (re: blocksize war).

If you are serious about defeating rival cryptocurrencies, then the best way is to copy them! Just copy their open source code, and steal it for yourself!Now you have feature parity... forever... for free!

Finally, keep in mind that Bitcoin is more popular than Litecoin. To defeat BTC, I ask you to consider wisely your strenghs and weaknesses.Bitcoin's weakness is its overconfidence and complacency. BTC may soon have drivechain itself — rending LTC obsolete. Instead, imagine a future where LTC activates first, and then pulls supporters and innovators from BTC to LTC.

It may cause a cultural death spiral at BTC. Then if LTC is the first drivechain-coin, that may give you your best chance at "hyper-Litecoin-ization", and a price of $4-5 million per LTC (instead of $0 -- which is where you are headed if you sit idle).





Vlad: *Why do you believe that activating Drivechains on Litecoin is a good idea? What does this mean for the future of the project?*

Paul: (answered above)

Vlad: *Litecoin already has MWEB — the MimbleWimble Extension Block, which adds privacy and scalability. Do you envision any opportunities to swap between MWEB LTC and Zcash LTC for better privacy, or simply to peg into sidechains directly from the extension block?*

Paul: MimbleWimble is fun, but (as I understand it) it does not significantly improve privacy nor scalability. What it does improve, is initial block download. The privacy "benefits" are defeated if an adversary spins up a bunch of LTC nodes, listens to everything, and logs everything. Thus the bad guys remember all the "deleted" txns — making MW not useful for privacy.

Similarly, the MW transaction cut-through does shrink txns (and the blocksize), but only after these are widely broadcast and processed in real time. So, if you were tunneling into the earth, it would NOT improve the speed of the drill: it only improves the time traveling between the surface and the drill point. You will not actually get through the mountainside any faster.

Drivechain in contrast offers zCash-style privacy and unlimited L2 transaction throughput.

Vlad: Why should Ethereum smart contract and application builders migrate towards Litecoin's sidechain? What are their main benefits compared to other chains?

Paul: Most of the ETH people own ETH — so they want ETH to succeed, not LTC. They will not surrender so easily.

But DC does allow you to tell a *new* potential user: "LTC can do anything that ETH can do". Thus you might persuade them to join LTC instead of ETH.

Vlad: *When do you believe Drivechains will get activated on Bitcoin too? Do you think that the Litecoin activation would disprove some FUD, just like the SegWit activation did back in 2017?*

Paul: Probably later this year.

Some? Yes.

Vlad: *In the event that miners decide to become evil and not release the users' funds, what are the leverages that user nodes have in order to punish this bad behavior?*

Paul: Users can bully miners around, via soft forks — but this is costly and expensive, and not worth it.

DC assumes that the L2s will generate fee revenue for miners. Kind of like opening a new restaurant.

So this question is like saying "In the event that the restaurant sucks and serves bad food, what can we do to make sure we get the food?". The better thing would be to just write the idea off, as a failure, and stop going to that restaurant. Depositing to any L2 (including drivechains) is a risk. Consider the tradeoffs before depositing to any L2.

Vlad: *As a Bitcoin maximalist, do you believe that the future might still be multi-chain and include Litecoin in it?*

Paul: Multi-chain? Yes, of course.

Multi-coin? No. I think it is a winner-take-all situation. If Litecoin is in the future, it will be because everything else (including BTC) is dead, and at $0/coin. That would be a great victory for mankind, although it would be puzzling in a few ways.

Vlad: *How can people read more about Drivechains and test some of the software?*

Paul: *drivechain.info*
LayerTwoLabs.com/download


#PAYWITH
#PAYWITH
#PAYWITH
#PAYWITH
#PAYWITH
#PAYWITH
#PAYWITH


LITECOIN
LITECOIN
LITECOIN
LITECOIN
LITECOIN
LITECOIN
LITECOIN

HOW TO RUN *and use* YOUR OWN LITECOIN CORE NODE

"you're not a first class Litecoin user until you spin up your node"

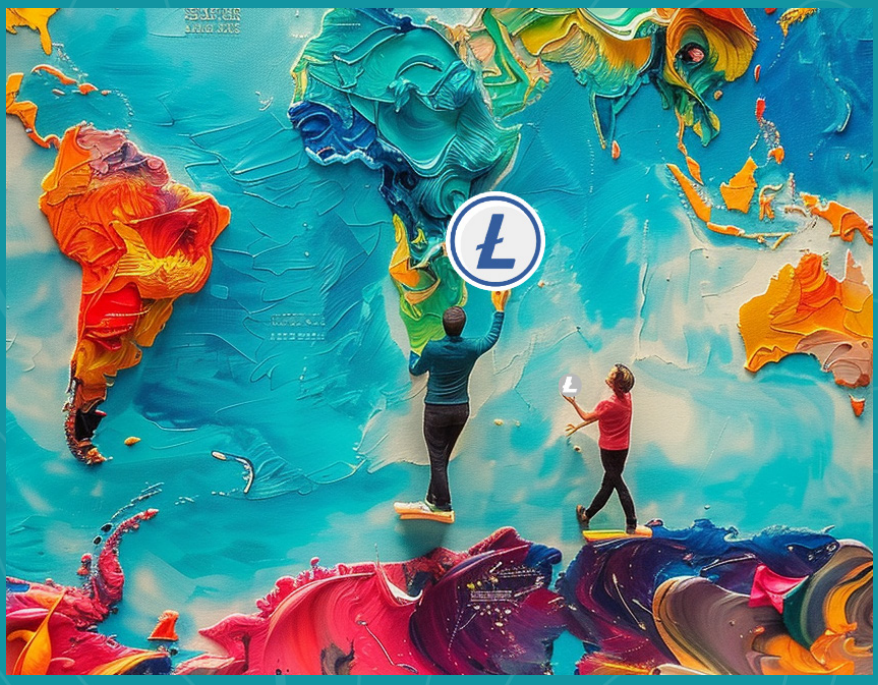
Running your own node is one of the biggest super powers that you have in Bitcoin and Litecoin. You get to validate your own transactions, you keep the miners honest, and you also have some privacy benefits — your wallet's public key doesn't get shared with someone else's server, so nobody else can know which transactions and addresses belong to you unless you voluntarily reveal it!

But most importantly, a Litecoin full node gives you the ability to try the latest features before everyone else: MWEB, ordinals, runes, and everything else that's coming. Since Litecoin Core is the most important piece of software in the ecosystem, it's the most battle-tested and developed one — to the extent that it can take the other wallets years until they catch up with the latest developments.

To put it plainly, you're not a first class Litecoin user until you spin up your own node and actually use it. The good news is that, if you're reading this, you most likely already have what you need in order to enjoy the fully sovereign and much more private experience.

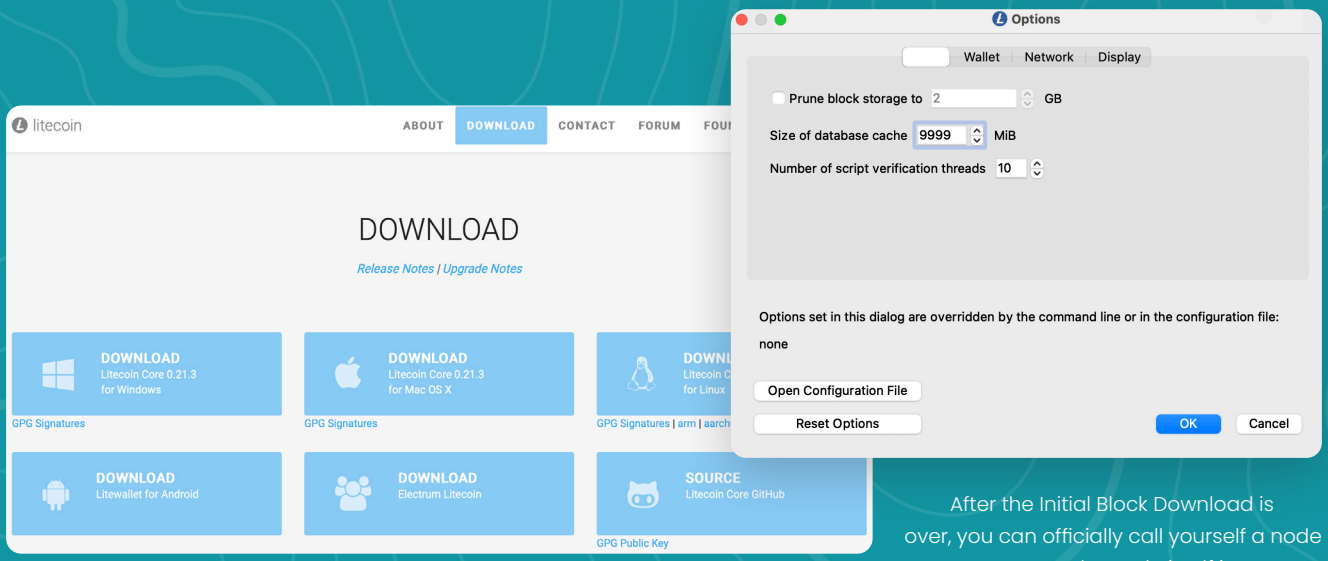
If you own a computer that's newer than 10 years and have access to the internet, then you already have the power! All you need to do is head over to litecoin.org and click on the "Download" button on the top menu. Depending on the operating system that you're using on your computer, you can opt for Litecoin Core on Windows, MacOS and Linux.

While the principle of "the best computer for a node is the one that you already have" applies, it's highly recommended that you run the Litecoin software on a user-friendly Linux distribution such as Ubuntu or Linux Mint. Apple's MacOS is the second best in terms of security, as it's UNIX-based and has a much better record of patching security exploits. While using Windows for your Litecoin node is possible, it's also the least secure approach — there's so much malware that's created every day for Microsoft's OS that it's probably better to dual boot Linux on your PC. It's not difficult, there are hundreds of tutorials on YouTube that will show you how to do it, and it can be an educational experience for those who are just dipping their toes into the world of free open source operating systems. If you don't feel comfortable doing this on your home or work computer, you can pick up an old laptop, format the hard drive (if you're paranoid, you can replace it entirely!), and then do a clean installation of Linux Mint — they made it so similar with Windows in terms of user experience, that you won't even realize that you're using something new!



Once you figure out the hardware and a software, it's time to ask yourself this: do you want to run a full archival node or a pruned node? The former will store on your hard drive the entire history of transactions on the Litecoin blockchain, from its creation in October 2011 and all the way to present. In total, you will need at least 91 GB of storage on your hard drive — if you don't have it, you can buy an external SSD for the purpose of storing your new node's data. On the other hand, a pruned node allows you to decide how many gigabytes of the entire blockchain you will be storing on your computer. There is no difference between the two approaches in terms of validation and time: they will perform the same task, except that the pruned node deletes older blocks while adding more recent ones.

Even on a low-powered device such



as the Raspberry Pi 4, syncing a full Litecoin node from genesis block shouldn't take longer than a day. All you have to do is leave the computer on running Litecoin Core, and make sure that your internet connection is always enabled.

But if you do care about sync time and you own a more powerful machine, here are a few tricks to speed up your initial blockchain download (IBD):

01 After downloading Litecoin Core, run the software.

02 Open the Options menu (also available as Preferences) and, under the Main tab, boost the size of the database cache and increase the number of script verification threads. For example, if your computer has 16 GB of RAM and the processor benefits from 32 threads, you can pump the default values to 9999 MiB (almost 10 GB of RAM) and 30 threads (assuming that the other 2 are necessary for the operating system to run smoothly). Sometimes the default 480 MB for the database cache and 2 threads for the processor are more than enough for a speedy sync — but if you use more of your computer's capacity, you will effectively shorten the waiting time.

03 Restart the Litecoin Core client by shutting it down and starting it up again.

04 Enjoy a much faster syncing experience — allowing the Litecoin Core client to use more of your system's resources will help you validate and download the entire blockchain history much faster. Sure, the bottleneck may be something like your slow internet connection. But it's important to understand what your computer can do and make sure you're using its resources at a reasonable capacity.

05 Once you sync a node, you can copy the block files to an external drive and reuse them for instant synchronizations in the future. Just navigate to the Litecoin installation folder, then backup the files you find in "Blocks" and "Chainstate". If you're sure that this first initial blockchain download was pure and untampered with, you can reuse the block data in the future to significantly reduce the waiting time. You can also transfer these files across multiple machines, even if the operating systems are different.

06 If possible, connect your computer via ethernet cable. While WiFi is more convenient, it's also slower and less reliable than the good old cable that goes into your network adapter. Sometimes, it's your internet speed that becomes the bottleneck for full node synchronization performance.

After the Initial Block Download is over, you can officially call yourself a node runner. However, the node itself is pretty pointless if you don't use it. So make sure you send and receive transactions from Litecoin Core — and whenever you can, peg your coins into MWEB to increase privacy and fungibility. All you have to do is go to the "Receive" tab, tick the "Generate MWEB address" box, and then click on "Create new receiving address". Copy this address (it must start with the distinctive prefix "ltcmweb"), then switch to the "Send" tab and paste your MWEB address to the "Pay To:" field.

If you want to select which UTXO (basically a wallet pocket which is distinct from all the others) will get pegged into MWEB, then open the "Preferences" menu and navigate to the "Wallet" tab. Here, you must tick the "Enable Coin Control" box and hit the "OK" button. Now the "Send" section of the wallet will include a new button called "Inputs..." which allows you to see every individual UTXO in your wallet. Pick which one you want to peg into MWEB (you can select multiples, but it's generally bad for privacy to create a link between two of your UTXOs because you narrow down your deniability), then double check that the MWEB address you pasted is correct and set the transaction fee (generally, 0.001 LTC per kilobyte is enough for a next block confirmation; but just to be sure, verify the recommended fees on a block explorer such as litecoinspace.org and blockchair.com/litecoin — you can also use your own node's estimation to determine the correct next block fee, but checking with third party sources can be a good idea for finding objectivity).

Once you entered all the details, double check the input data and hit "Send". You will see a final screen which tells you how much LTC you're sending, to which address, and how much you're





paying in fees. If everything is correct, proceed to confirm — this will sign and broadcast your transaction across the network. If you're using this process to peg into MWEB via self-transfer, your node will also instantly notify you about the incoming transaction... and within a few minutes your LTC will have enough confirmations to be safe to spend. Next time you make a transaction, make sure you choose your MWEB inputs (unless you're dealing with a very strict KYC exchange that demands absolute transparency for the origin of your funds). Remember that increasing activity and demand for MWEB will normalize the use of privacy in general and create a much healthier culture which opposes an Orwellian future.

Another useful way to integrate your node into your daily transaction flow is to take the IP address of your Litecoin Core node and paste it into Litewallet for a serious dose of sovereign mobile use. In your Litewallet phone app, go to Menu —> Settings —> Advanced Settings —> Litecoin Nodes —> Switch to Manual Mode. Next up, type the IP address which points to your node and you're good to go! However, remember that you will have to keep the computer node online every time you want to check your balance or send transactions from Litewallet. Sovereignty is not always the most convenient approach — but if you care about privacy and decentralization, you should make an effort towards it. After all, you don't need to keep your Litecoin Core node online 24/7: just make sure you start it up when you're about to use it.

Keep in mind that this doesn't only work with Litewallet — I've only recommended the most popular mobile wallet, which benefits from active development. Any existing or future mobile wallet that's dedicated to Litecoin should enable you to change the SPV server. It should also be noted that the BitBox02 hardware wallet features a native desktop and mobile app that lets you make use of your personal Litecoin node. Don't underestimate the sovereignty you can get from this type of setup — and if you order a BitBox02 and wish to get a 5% discount, use promo code BTCTKVR at checkout.

For those who want to take a deep dive into setting up home nodes to include port forwarding and a static IP address (very useful for using on a mobile wallet or on a hardware wallet such as BitBox02), you should definitely check out the excellent guide published at lookintolitecoin.com/fullnode. The article URL has also been saved on the WayBack machine, so you can type it in the archive.org search box even if the website goes offline. If you need more advanced features, you might need to look into Electrum servers (an extra indexing layer that can be used to power up SPV wallets).

Your Litecoin Core node can also be used in the context of minting ordinal inscriptions and etching runes — as a matter of fact, the ord software client requires it. Inserting arbitrary data into the blockchain through these protocols can only be performed in the presence of a full node. So if you're already running one, then you can start a fun project through which you create collectibles that will forever exist on the Litecoin blockchain. Just keep in mind that ordinals are a non-monetary use of the block space, so don't abuse them to the point that you make transaction fees high and validation slow for everyone else — however, such a feat requires you to pay a lot of LTC in transaction fees and the Litecoin miners would most likely feel very happy if there was more demand for block space.

Litecoin Core is the software where all the significant upgrades happen first. So if you're serious about your sovereignty and wish to explore the Litecoin ecosystem in the most uncompromising way out there, you should definitely sync one as soon as possible. It can be a fun and educational weekend project that will help you understand why decentralization matters and why this money network is unstoppable. Have fun staying sovereign!

We love Bitcoin

We love Litecoin

We love UTXO

We love POW

We are Alephium.

We also do sharding, smart contracts, more efficient mining, and have a novel VM, plus lightweight nodes for decentralization.

CHARLIE LEE QUOTES

ABOUT MWEB, LITECOIN & PRIVACY



Bitcoin Takeover Podcast, S15E34

"I think financial privacy is a human right. You should be able to spend your money without everyone knowing how much you have or who you're sending money to." (00:16:48)

"Putting everything on the base layer is not the most efficient solution. It doesn't scale. It scales linearly. And you want something that scales exponentially." (00:06:53)

"[MWEB] is at least doubling the block size. But Litecoin blocks aren't full, so it's not something that's needed, but it's something that is ready to be used if people start using more of it." (00:14:56)

"Confidential transactions are a way where transaction amounts are blinded, so they're hidden from everyone else other than the recipient and the sender." (00:20:34)

"MWEB gets you most of the way there, 90% of the way there, and that's good enough for the majority of users." (00:32:58)

"The most important thing is just enough financial privacy where people you interact with can't easily tell how much money you have." (00:34:32)

"The other thing that MimbleWimble does is something called cut-through. Every transaction, with all the inputs and outputs of a transaction in a specific block, gets added together into one large transaction with hundreds of inputs and hundreds of outputs. And if anything cancels out, they're just dropped from the blockchain altogether without even saving it to the blockchain. Specifically, what that means is if, for example, I sent you one litecoin and then you immediately sent that one litecoin to someone else, then all that matters is that the final recipient received one litecoin. So the transaction to send one litecoin to you and for you to send one to the final recipient can totally be dropped from the blockchain. That's one of the unique features of MimbleWimble: it's »





the ability to collect all the inputs and outputs and drop whatever it cancels out. That adds a bit of privacy to the blockchain because transactions that are cancelled out are just totally gone and never recorded. And the other thing about MimbleWimble is that it makes it very easy to do something like a CoinJoin because the amounts are not public. They're blinded, so it's easier to do CoinJoin where you just combine all the inputs and outputs into one huge transaction and submit that to the network." (00:23:56)

"The thing with MWEB is it matters how much usage there is, right? Right now there aren't a lot of peg-ins and peg-outs. So when you move coins from the mainchain to MWEB, it's easy to see that you move the coins — because on one side it's totally transparent. So if I sent five litecoins to MWEB, you can kind of track that, right? So, like most privacy technology, more people using it improves the effectiveness of having this financial privacy." (00:25:07)

"Our developer, David Burkett, worked on Grin++ and he was able to come up with a solution so that there are addresses and there are ways to send coins to an address as opposed to needing both parties to be online to negotiate the transaction. So I think that's something that's very important. One of the features of Bitcoin is that you can send coins without the recipient being online and without needing to communicate with the recipient... unlike Lightning Network, where you need to do something like that. So having that feature on Litecoin with MWEB, I think it's a huge breakthrough. And it's huge! Thanks to David Burkett for coming up with a way to do that for our implementation." (00:30:42)

"I don't see Bitcoin adopting MWEB anytime soon. Bitcoin is probably a little bit too conservative to do something so drastic. But suddenly you have something like this work on Litecoin, and you show that it is possible to improve fungibility and privacy on a coin similar to Bitcoin by basically taking a different kind of tradeoff than what Bitcoin is doing. And it's a good, good place to experiment." (00:40:09)



"To be honest, I haven't really looked into it [BIP300] that much. We've been currently focused on MWEB. But it's something that people have proposed to test on Litecoin, and I'm perfectly fine if they want to do that. And I'll work with them to see how we can support and help test Drivechain on Litecoin." (00:47:47)

"I didn't expect people to use litecoin more than bitcoin on BitPay. Yeah, I actually never expected that to ever happen. but it just proves to people that LTC is a very useful currency for payments." (00:50:55)

Listen to the entire interview or watch it on YouTube!

LITECOIN *and the* LIGHTNING NETWORK

"...one of the most exciting breakthroughs in the history of cryptocurrencies."



The Lightning Network is one of the most exciting breakthroughs in the history of cryptocurrencies. Before it, the largest majority of improvement ideas revolved around increasing the throughput of blockchains or adding other blockchains on top. But Lightning's design enables transactions between peers at the speed of the users' internet, with instant settlements and very little trust involved. In other words, it's a much more elegant design which scales better than any blockchain simply because it no longer requires the entire network to store and verify everyone else's transactions.

However, the Lightning network comes with quirks and intricacies of its own. If you don't understand how it works, here's a brief metaphor: Lightning nodes are like separate islands that are spread across a vast sea. In order for these islands to communicate with each other and engage in trade, they must build one-way bridges: so if island 1 wants to sent money to island 84, then island 1 must build a bridge to island 84; but if island 84 wants to also send a transaction to island 1, it can't use the same bridge... so it must build a bridge of its own. In the Lightning context, these bridges are referred to as "channels".

This is just the simplest example, which involves two parties which directly transact. But these islands usually conduct trade with lots of others — so it's not always necessary to build new bridges, as there might be common connections whose architecture can be used. So if island 1 already built a bridge with the Litecoin Foundation while the Litecoin Foundation previously built a bridge to island 84, then the financial transaction can be relayed through the Litecoin Foundation. Since it provided a service through its infrastructure, the Litecoin Foundation will collect a small routing fee. We can also think of more intricate examples involving dozens of participants, and this situation leads to the kind of competition where the fastest route with the best connections will collect more fees.

The Lightning network was presented as a scaling solution for Bitcoin, but it's blockchain-agnostic: meaning that every network that's compatible with Bitcoin can add it on top. Litecoin never had a scaling debate and doesn't really need this type of layer two.. at least, not yet. But there are still some privacy and speed benefits that Lightning offers, which can get complemented by atomic swaps across chains: basically, users can build decentralized and non-custodial exchanges through which they can trustlessly trade between BTC and LTC. The only reason why these were not standardized yet is that there wasn't much demand for

such a feature, as regulations regarding centralized solutions weren't strict enough to incentivize such a development.

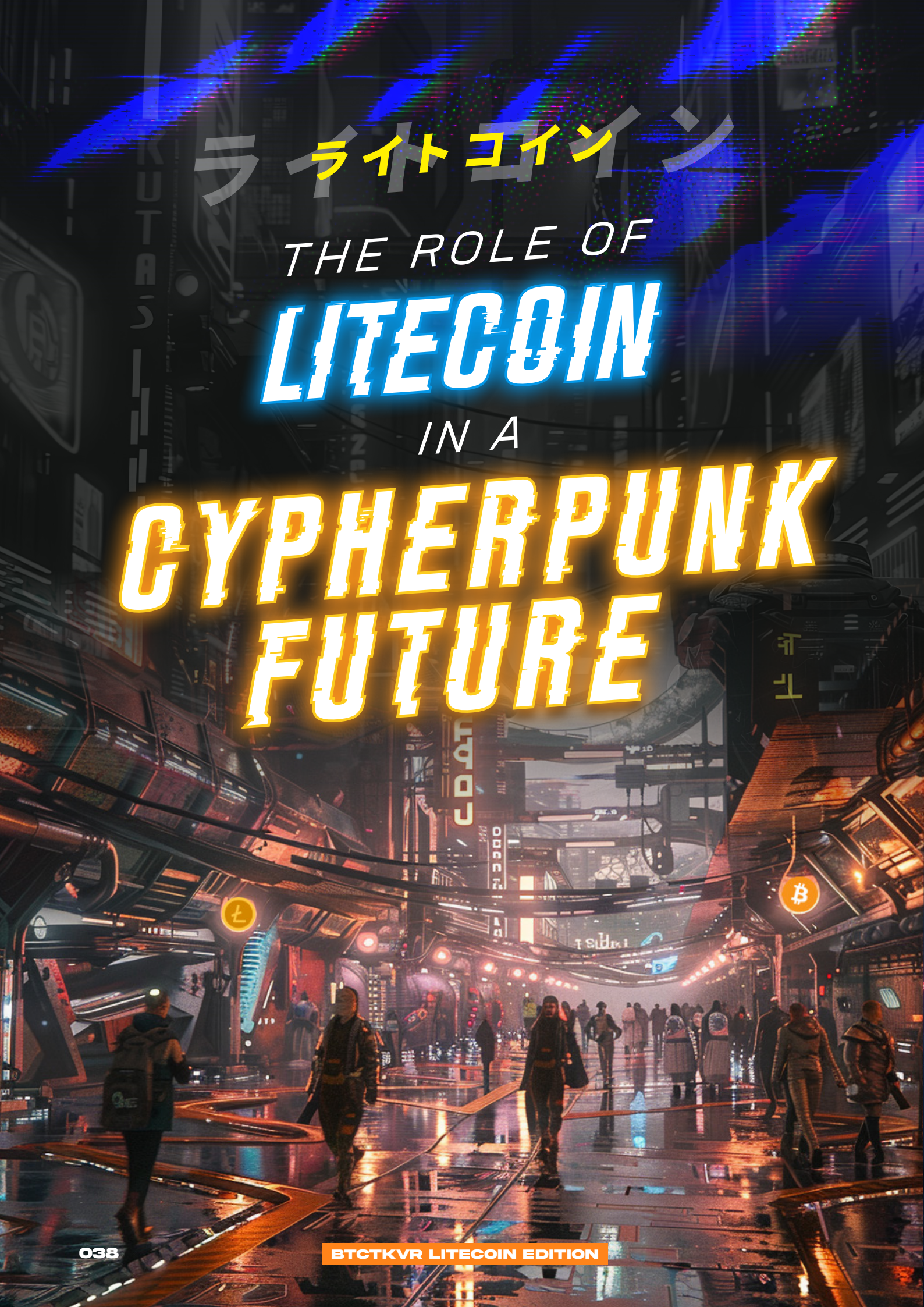
As of May 26th 2024, Litecoin's Lightning network only has 95 nodes which opened 170 channels between each other. The capacity locked adds up to 35.27 LTC, which means that the adoption didn't pick up too much. However, Litecoin has hosted Lightning network projects on main net for longer than Bitcoin did: back in early 2017 when using Lightning was deemed too "reckless" for Bitcoin, developers from Lightning Labs (creators of lnd) and ACINQ (creators of Phoenix wallet) were experimenting with features on Lightning, transacting LTC between one another.



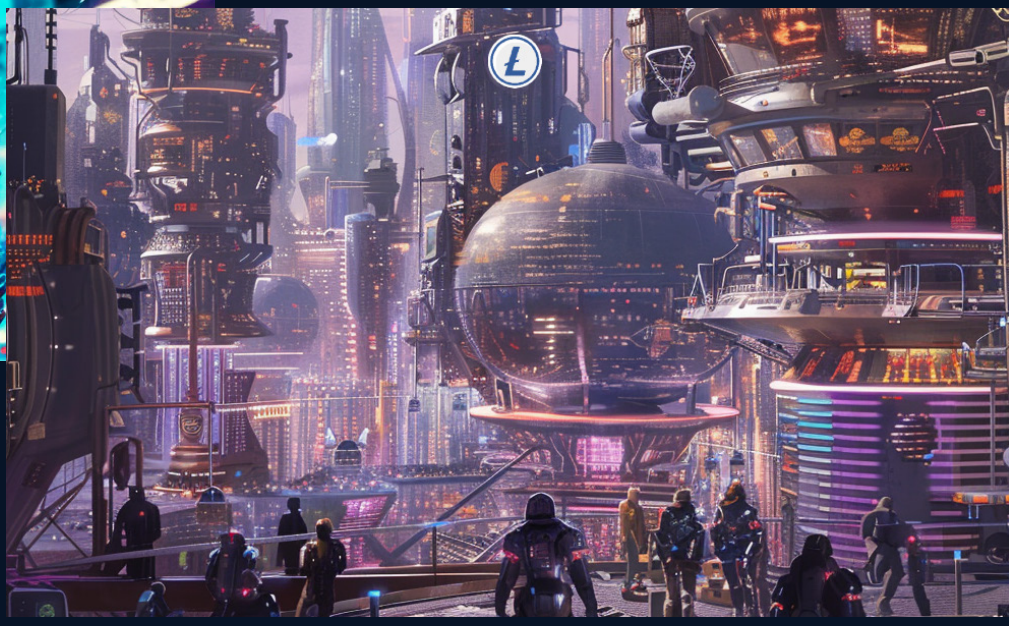
As on-chain transactions become more expensive over the years, it's very likely for Lightning on Litecoin to witness a resurgence. By then, the development of the second layer will have become much more mature, with many of today's quirks and shortcomings being fixed in a way that makes deploying and operating a personal node more easy. For now, running Lightning on Litecoin doesn't make much sense — especially when you're using MWEB for fungibility and while the transaction fees are negligible. But the use case of doing atomic swaps between BTC and LTC might become a serious catalyst towards LN adoption. Here's a personal story: back in March or April 2018, I followed a Lightning network setup guide by legendary Litecoin contributor ecurrencyhodler and burned my SSD in the process. It wasn't the fault of Lightning per se — probably any demanding application would have caused the same damage. But it's a memorable story which reminds me of the thrills of being an early adopter.

Charlie Lee, creator of Litecoin, also referred to the Lightning network whitepaper as being the second most exciting scientific paper about money that he read since the release of Bitcoin. In October 2018, he also tweeted: "Bitcoin with Lightning Network more closely fits the Bitcoin whitepaper's title: 'A Peer-to-Peer Electronic Cash System'. This is Satoshi's Vision." As he frequently acknowledges in interviews, he is still an investor in Lightning Labs and other companies which use the Lightning network for payments. So he's definitely onto something, though it might be a little too early for the rest of the world to realize. There's a storm coming soon, and all freedom lovers are bound to be struck by Lightning!




ライトコイン
THE ROLE OF
LITECOIN
IN A
CYPHERPUNK
FUTURE





In a cypherpunk future, the people possess the technological tools to gain more freedom from their governments. They can share encrypted data with each other, in a way that no state actor can effectively surveil and identify. They have the power to choose where they live, to the point where nation states become just like restaurants: all state entities display attractive menus, hoping that the customers would choose to enter, pay for the benefits provided, and hopefully stay. And most importantly, the same people are able to make financial payments that no government can control, censor, tax, devalue through inflation, or clearly link to someone's identity.

In other words, a cypherpunk future radically changes the nature of social contracts and constitutions. The focus is no longer on state actors, leaders, and a vague collective good — it's all about individuals, their best interest, and their choices. This cypherpunk future promotes freedom and the ability to peacefully opt out. It puts voting with one's feet (leaving any country with great ease) at the forefront of political decision making — after all, any polity loses legitimacy if there is nobody who grants permission to be governed. These ideas aren't as radical as they sound: not so long ago, our democracies were built on the principle of consent and no taxation without representation... but somewhere along the way, they forgot about the first convention between those who govern and those who are governed.

Today, we already have most of the tools necessary to build a cypherpunk future. We have the kind of cryptography that no government super computer can break. We have open source projects for everything, ranging from software to produce guns, automobiles, and genetic engineering. And most importantly, we have decentralized cryptocurrencies that are able to fuel this type of parallel economy and make any useful project prosper even if the political establishment removes it from the traditional financial system.

But technological advancements must be followed by a culture that protects and nurtures them. For this, we need philosophers, artists, orators, and educators to create works that emphasize on the benefits of technologically-enforced freedoms. We also need well-funded software developers to work towards improving, optimizing, and ultimately revolutionizing the way in which we make financial payments to each other. Yet most importantly,



we need normal everyday people to use the technology and popularize its use to the point where it becomes unstoppable.

As Bitcoin's scaling partner and experimentation pioneer, Litecoin finds itself in a pretty good position: it's been around since 2011 and has a large community of users, which makes it robust and resilient; it's the leader among Scrypt coins, which means that the likeliness of going through a malevolent 51% attack is extremely low; it's similar enough with Bitcoin to attract users and get integrated into various parallel payment systems, but also different enough to have a value proposition of its own; it has a higher transaction throughput than Bitcoin and also benefits from better privacy thanks to the MWEB activation; and most importantly, it follows a culture of progress and improvements which also benefits Bitcoin on the long run.

The fact that Litecoin's economic policy has remained a constant since 2011 is also a good sign: it shows that there's a degree of commitment in making incentives work, as the community is willing to find solutions to increase the demand for transactions.

Today, Litecoin is perfect for payments and for intermediating swaps between coins. It's thermodynamically safe thanks to the Proof of Work security, it's fast enough to attract use in commerce, and it has such a great network effect that you'll find it listed on every exchange and across virtually all ATM networks. For freedom lovers, Litecoin is an ideal tool: as it has pretty good privacy and fungibility, a degree of adoption that's second only to Bitcoin, and it's designed to remain affordable.



What about the maximalist thesis of "one coin to rule them all", though? After all, we can envision a future in which cryptography and computing become so advanced that Bitcoin can do everything. Both economically and technologically, a future in which only Bitcoin exists and thrives all alone is unrealistic. There will always be demand for features that aren't necessarily included in Bitcoin, and incentivized experimentation is the market's best evolution mechanism. Developers take greater risks and make more interesting discoveries when they can issue their own currency or token, as opposed to raising BTC and having to account to investors for it.

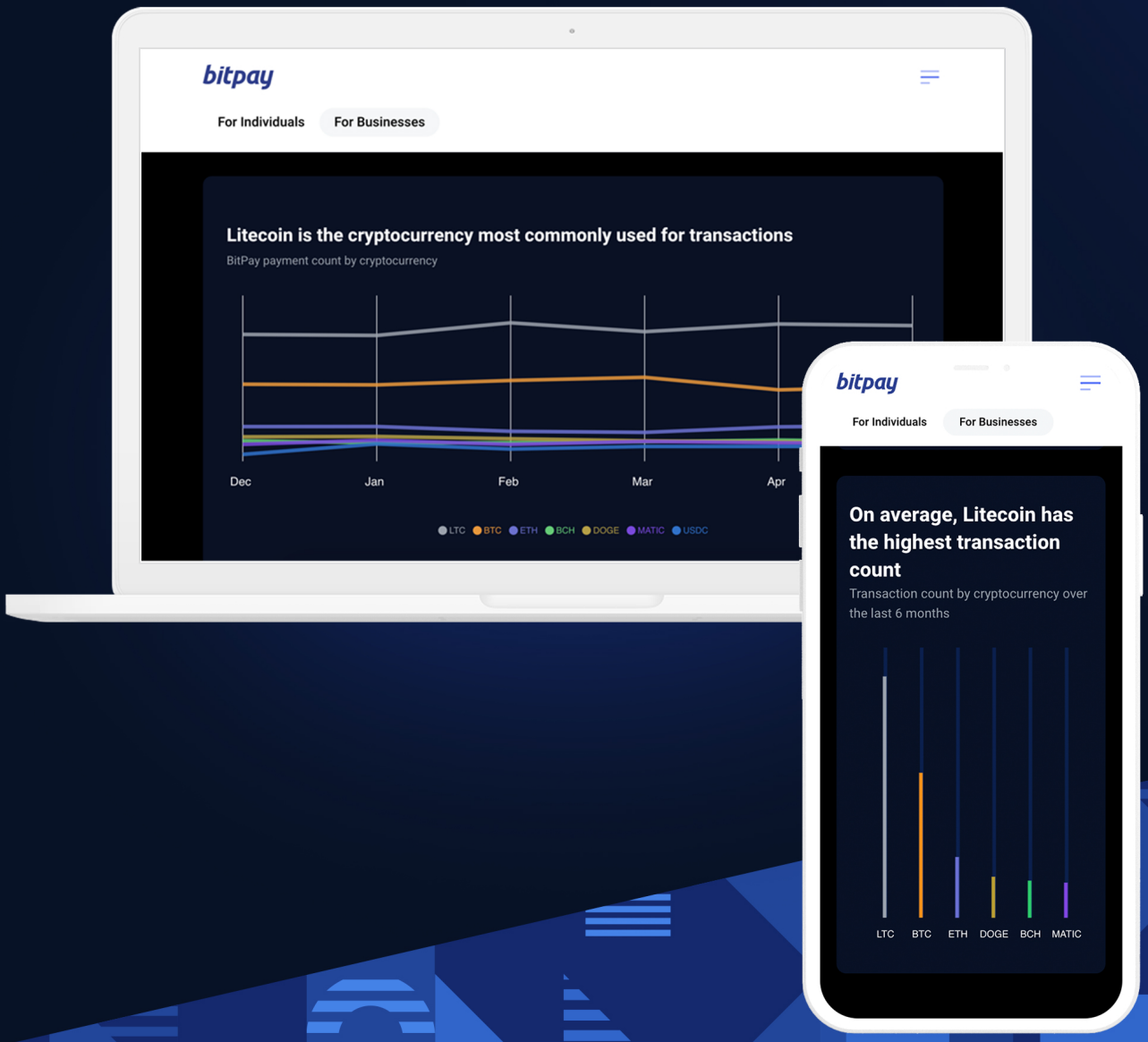
Furthermore, competition is useful because it pushes innovation and constantly raises the standard all across the board. In the event that certain governments become hostile towards forms of money that they don't issue and control, it's better if they have multiple targets to pursue — going after only one is extremely simple. Because even though Bitcoin and Litecoin transactions can't be censored, the censorship is still possible at the social level — users, miners, nodes, service providers, and developers are politically vulnerable.

By simply existing, Litecoin makes Bitcoin more resilient to human politics. It also provides a layer to scale peer to peer transactions, while simultaneously being more open to experimentation. The Lindy effects are also on Litecoin's side: having been around since 2011 and growing into the biggest Proof of Work coin for its Scrypt mining algorithm, it benefits from a thermodynamic security that's second only to Bitcoin's... but which doesn't rely on Bitcoin and is not vulnerable to malevolence from BTC miners.

In a cypherpunk future, Litecoin has earned its own seat at the table — and everyone who has the ability to understand this is very much ahead of his time.

bitpay

The leading crypto **payment processor** in the world



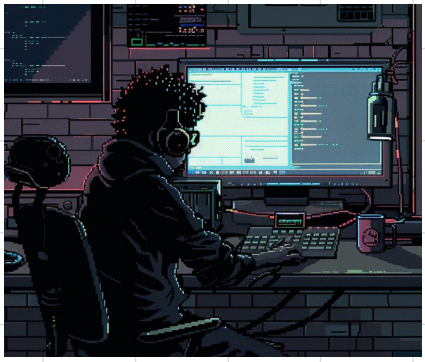
3 GENERATIONS OF LITECOIN DEVS



LOSHAN
Litecoin Core



KERRY WASHINGTON
LiteWallet



HECTOR CHU
MWEB

Vlad: *When did you start contributing to Litecoin and why did you choose this project?*

Loshan: And I've been in the Litecoin community since. As a community member, I wanted to do whatever I could to make Litecoin grow, so I was initially involved with stuff on Reddit and the original LitecoinTalk forums. Things like creating an animated 'What is Litecoin?' video for YouTube. After a while, I got involved in the Litecoin Association. I ended up running the @litecoin twitter account, inherited it around 3k followers, and was around 800k when I'd stopped.

Why I got into Litecoin development? At that time, there was no Litecoin mobile wallet. And I felt that it would be necessary for a mobile wallet if we wanted more people to use Litecoin. At the time, Apple didn't allow any crypto wallet apps... but once that changed, I started working on the original build of LoafWallet for iPhones (forked from BreadWallet). Working on that project was mostly how I learnt about the technical blockchain stuff.

Kerry Washington: I joined the Litecoin Foundation in 2017-2018 and I saw that I could help fix a lot of bugs in the Loafwallet code. It was also an easy way to keep my skills sharp.

Hector Chu: I started contributing when the MWEB testnet launched in the second half of 2020. I chose this project because I was a big fan of MimbleWimble and I wanted to see it implemented on what was at the time a top 5 coin.

Vlad: *How easy or difficult is it to build applications and integrations for Litecoin?*

Loshan: Not very difficult. Litecoin is very, very similar to Bitcoin. If you can theoretically do something on the Bitcoin network, you can probably do it even better with Litecoin! There are also many libraries that support Litecoin, like bitcoinjs, ltcsuite for golang, and an early implementation in Rust! Litecoin also supports more advanced non-digital money features or smart contracts like Ordinals Lite & Runes & OmniLite. More scriptable smart contracts are also possible with Litecoin Computer.

Kerry Washington: Well, most of the work was done. Loafwallet was published and the interface to manage Litecoin was working fine. There were and still issues in that in order to get better, you need more users and we were trying to replicate the 2018 boom while the user base was shrinking. Too many look at Litecoin as a speculative asset... and we suffered especially since our goal was to spread general adoption people won't blame us for the shortcomings.

They wanted a exchange interface first and people couldn't wrap their heads around the bigger picture.

Hector Chu: In theory, it is as easy as building for Bitcoin. But a lot of Bitcoin apps and libraries remain unported to Litecoin. So anyone who wants to build on top of them needs to do the porting.

Vlad: *Loshan, for years you have contributed to Litecoin Core and Electrum LTC. What was your favorite part in doing this job and what are some memorable challenges?*

Loshan: To clarify, I haven't done much work with Electrum-LTC. I'm taking over as the maintainer, though.

To me, my favourite part of the job is getting the things I built in to other people's hands! After months of working on something, it's always awesome to see the team's hard work pay off! Challenges: not being lazy. I get bored very quickly, at which point I start working on something else... and then I get bored and move on to something else. This is why I am often juggling with so many different projects — leading to projects taking much longer than I'd want.

Vlad: *For years, you have worked on LiteWallet — which started out as Litecoin Wallet and was initially a fork of Breadwallet. What was the biggest challenge that you encountered and how did you overcome it?*

Kerry Washington: Well it was actually called Loafwallet. Litewallet (lowercase w). The architecture in the IOS version

was a personalized state management system that comes from Redux and it was/is very unusual.

Also, the code and conventions taken were not the way most iOS developers handle challenges. Finally, there are many shortcuts that are generally frowned upon in iOS. These design choices really make the app fail silently....which is bad.

Vlad: *You recently brought MWEB to Electrum LTC and also made the privacy layer work on the Ledger Nano S hardware wallet. What motivated you to do this and how long did it take?*

Hector Chu: We were discussing in the chat about how we wanted to see every coin pegged-in to MWEB. Someone brought up that it wasn't possible unless MWEB could be used with hardware wallets. Another mentioned that it would be good enough for him if Electrum could be used with MWEB and Ledger. That motivated me to bring the work I did for LiteWallet MWEB to Electrum. In total the port took around 3 weeks, and the HW wallet support another 2 weeks.

Vlad: *What are you currently working on and what is next?*

Loshan: Currently working on building an app that makes Litecoin easier than ever to buy/sell/hodl/spend. Come to the Litecoin Summit if you'd like to see more about the future of Litecoin!

Kerry Washington: We are fully up and running on more outreach with Instagram, Facebook, and YouTube. We are also working on the UI/UX as a complete refresh. And of course, we are working on MWEB for mobile.

Hector Chu: I don't have a plan for another project right now. I've already worked non-stop these past 6 months and achieved all my goals already.

Vlad: *If you had unlimited time and funding to pursue a project in Litecoin, what would it be and why?*

Loshan: From a development point of view, the team's primary objective has been to grow adoption and the use of MWEB. Given unlimited money and developer time, I would like every wallet (on exchanges/mobile apps/ATMs) to support MWEB. New additions can also be made to improve MWEB privacy.

One of my personal goals is to increase Litecoin usage by 'maxis' and 'shitcoiners' — I think Litecoin has a unique advantage of high volume, liquidity and stability. We can use Atomic Swaps to make Litecoin play a more prominent behind the scenes roles of payments in other networks.

Kerry Washington: More marketing to general public. Let's face it, the one thing crypto projects are good for is spending a shot-ton on marketing... and it works really well for the developers who then rug pull their users.

Our entire revenue (partner revenue, service fees, donations) still amounts to less than annual USD figures. So we just have little ability to compete in the users' mind space

We do need to expand the dev team and 2 part time devs for iOS and Android would be nice, but even freelancers run when they see the complexity of the code. Two moderately decent developers would 3x our costs... and we don't have the resources

Hector Chu: There's still some more work that can be done to break the links in the transaction graph. I don't remember what the various proposals are called. A lot of people complain that MWEB privacy as it stands today doesn't hide the transaction graph (the links between inputs and outputs).

Vlad: *If someone wants to start contributing to Litecoin software today, what is the best place to start?*

Loshan: Honestly, the best place to start is to go to our bounties website *(https://lite.space)* and try to pick a bounty that's open. If there's something you're interested in doing, and that's not a bounty, please contact us and we can connect to help set up a bounty and help you get onboarded to develop apps for Litecoin.

Kerry Washington: Writing for mobile apps is simply not the same as blockchain. You can't just open a PR and expect someone to accept it into the code base. There needs to be more planning and management because publishing requires many moving parts.

We always encourage people to apply to the team, start contributing as a teammate. Not work as a wolf, then bounce.

Hector Chu: It's a bit hard to know the best place to start, you kinda have to be a self-starter and read a lot of code as the documentation is very bad. Also, do they want to contribute to Litecoin Core or the apps in the ecosystem? Unfortunately, I don't have a good answer for this question.

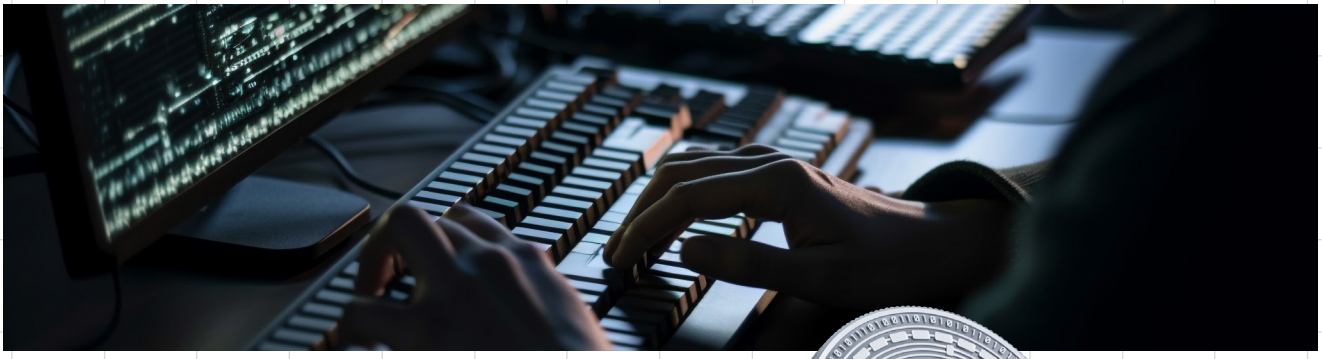
Vlad: *What's your price prediction for Litecoin during this bull market?*

Loshan: Bull market, what bull market? lol. I don't speculate on the price.

Regarding adoption, analytics from us and third-parties (BitPay & Coingate) show that Litecoin usage is increasing. To be honest, Litecoin is pretty much one of the few cryptocurrencies which make sense as "digital money".

Kerry Washington: I don't do price predictions Any other prediction regarding adoption? General adoption will boost price!

Hector Chu: Litecoin should be over a 1000 $. Adoption is already coming along nicely as others will point out with the metrics.





How to mine LITECOIN *and Dogecoin*





Mining Litecoin is one of the 4 most significant ways in which you can contribute to the money network's success and well-being — the other 3 being developing software, running your own fully validating node, and increasing adoption by spreading the word, creating educational resources, and using the currency as often as you can to send and receive payments.

However, it's also a technical and somewhat intimidating endeavor which most users leave to specialists. This article aims to convince you to consider mining Litecoin (and Dogecoin). It also presents all the information you need to get started.

First of all, what is mining and what is the point of it? Well, Proof of Work cryptocurrencies need a decentralized network of miners in order to be secure against double spend attacks. In the absence of a central entity to establish what is valid and what is not, the role of establishing truth is fulfilled by network nodes (which store the ledger of transactions, validate incoming transactions, and relay the data to the miners) and miners (specialized computers that search for the unique hash in order to discover a block and collect the monetary reward).

Through mining, Litecoin gains thermodynamic security. Therefore, the act of trying to attack the network implies a cost in electricity that is usually much higher than simply playing by the rules to obtain financial rewards. In the event of forks and social attacks, mining also helps in determining which one is the real chain: it's always the longest chain, with the most amount of Proof of Work.

As electricity gets converted into litecoins, the digital money also gets a base valuation and somewhat of an intrinsic value: in a healthy economy where there is enough demand for the existing supply, the price will rarely dip below the average production cost. Of course, we're not talking about an implementation of the Marxist labor theory of value — it's just that market participants assess value according to the utility that a decentralized form of money has for them. The fact that they don't want to let it become unprofitable to produce is a good sign, but not something that should be taken for granted.

Secondly, it's worth noting that Litecoin uses the Scrypt mining algorithm. It differs from Bitcoin's SHA256 because it's much more memory-intensive, and was originally thought out to allow GPU miners (who were made unprofitable on Bitcoin by FPGAs and ASICs) to continue hashing. In the meantime, ASICs were also created for Litecoin's Scrypt — so today, the most efficient way to mine is to buy one of these specialized devices.

Can you still use your computer's resources to mine with the general-purpose hardware you already own? Of course, but your effort will be extremely inefficient and your lottery ticket will have much worse odds than even the most affordable ASIC machine on the market. But if you do want to mine with your computer and receive LTC, you might want to look into NiceHash.

Thirdly, it's very important to know that Litecoin miners have had the option to merge-mine Dogecoin since August 2014. In the beginning, the benefits of setting up DOGE mining were barely significant. But today, in the era when Elon Musk popularized the world's best-known Shiba Inu currency to the point that Tesla accepts it in their merchandise store, merge-mining is a must. This is also the reason why pretty much all mining pools have integrated merged mining by default: the extended profitability currently pays for the network's security budget.

So you decided it's time to start Litecoin and Dogecoin mining? Well, there are two very important decisions to make: the hardware that you will be using and whether or not you will collaborate with a mining pool or go solo.

Today, there are dozens of Scrypt mining machines from which you can choose. Depending on the amount of energy you can afford to use and the heat/noise you're willing to tolerate (or else acoustically isolate), you have industrial-scale devices and tiny specialized computers that are made for home use. Sure, you can still mine with your CPU or GPU... but it's extremely inefficient compared to a much more affordable ASIC.

Even the most underpowered ASIC will be better at hashing Scrypt than the high-end Nvidia or Intel/AMD chips. You can't beat specialization with general-purpose hardware. For instance, the Lokotech S1 Hashblade (which you can mount in the video card slot of your computer) will make an RTX 3090 Ti video card look like a toy — and it's about 25% cheaper too! But then again, even a tiny Goldshell Mini DOGE III should perform much better (more hashes, smaller electricity consumption) than the Nvidia graphics card.

Of course, you can use your video card to mine via NiceHash and receive LTC payouts. But you're not mining Litecoin and you're not granting the Litecoin network any security benefits with your contribution. Instead, NiceHash decides which cryptocurrency is most profitable for your chips to mine, sells the hashrate to somebody who is interested in boosting their security, then sends you LTC and takes a cut for intermediating the business. It's not the ideal way to mine, but if you only have a GPU and want to earn some litecoins, then it's probably better than running Scrypt cycles in an inefficient and uncompetitive way.

In the table below, you will find some of the most popular ASIC miners for the Scrypt algorithm. These devices will merge-mine both LTC and DOGE. The ASIC prices and probabilities reflect the values on July 1st 2024, when the average hash rate is that of **891.1 TH/s**.

For determining probability, the following formula was used:

Global Litecoin hash rate: 891.1 TH/s = 891,100 GH/s
Miner's share = Miner's hash rate / Global Litecoin hash rate = X / 891.100 GH/s
Probability = Miner's share of hash rate * Blocks mined per day (24 hours * 60 minutes / 2.5 minutes = 576 blocks)

Keep in mind that the ASIC prices will keep going down as more innovation happens in the chip manufacturing industry, while the probability to solo mine will diminish as hash rate increases. In some cases, it might also be a good idea to buy used mining machines from professional farms that upgraded their rigs — if you don't want to commit a lot of money when you first start your hobby, it's a good option. Just make sure that you buy something that functions within the specified specs and doesn't show signs or wear and tear.



	HASH RATE (Gh/s)	POWER (W)	POWER EFFICIENCY (J/Mh)	PRICE	PROBABILITY TO SOLO MINE A LITECOIN BLOCK IN 24H
Lokotech FullStack	23.96	2040	0.0853	$20199	0.0154%
Bitmain AntMiner L9	16	3360	0.21	$11200	0.0103%
Goldshell LT6	3.35	3200	955	$10799	0.000216%
ElphaPex DG1+	14	3920	0.28	$10700	0.0091%
ElphaPex DG1	11	3420	0.31	$7500	0.0071%
Bitmain AntMiner L7	0.9	3260	0.36	$6335	0.000057%
FusionSilicon X6	0.86	1079	1.255	$4449	0.000055%
BW L21	0.55	950	1.727	$4349	0.00035%
InnoSilicon A6 LTCMaster	1.23	1500	1.22	$2799	0.000079%
Lokotech S1 Hashblade	1.99	145	0.0726	$1799	0.000128%
Goldshell Mini DODGE III	0.7	400	0.57	$759	0.000045%
Bitmain Antminter L3+	0.6	850	1.42	$500	0.000038%
FutureBit MoonLander 2	0,005	10	2	$200	0.00000032%

How hard is it to connect your ASIC miner to a pool? It's no biggie: after you plug the device to your home router via ethernet cable (recommended due to better stability and no variance of signal strength), you switch it on and use your computer to scan for the IP address of your miner on the home network. Programs such as Advanced IP Scanner (on Windows) and Angry IP Scanner (on Mac and Linux) will help you identify the address of every device that's connected to the same network. The IP should look like this: 192.168.1.X (X being the unique number that's associated with your miner).

Type that IP address into your internet browser's address bar, then hit the "Go" button and you will be greeted by the interface of your ASIC miner's firmware. In most cases, you will be asked to type the username and password — both of which you should find in the device's instruction manual or on a label that's attached to the back of the machine. Afterwards, configure how your will be mining (solo or exchange) and to which address your want to receive your LTC (preferably, use a full node wallet that you back up properly).

As you can see in the chart, not even the most powerful ASIC miner can guarantee the discovery of a block within 24 hours. Sure, your chances are pretty high with something that outputs more than a dozen gigahashes per second, but there is never any guarantee of payout. This is why mining pools were invented: to collaborate towards finding blocks, to split the rewards according to individual contributions, and to offer a more consistent and predictable pay even when the luck runs out for a while.

Essentially, solo mining is like buying lottery tickets — the more terahashes per second you purchase, the higher your chances to win the jackpot become. But if you're serious about being a full-time miner, then it's probably a good idea to compromise a little bit on the reward size and opt for more regular small rewards instead.

But how will you choose from the dozen of Litecoin mining pools? Well, there are multiple factors that you must weigh in: the minimum amount that you must withdraw (basically how much you have to commit to work with the mining entity before you request a payout), whether or not you will be merge mining Dogecoin to increase revenue, where the pool is located (very important for censorship resistance and geopolitical game theory), to which extent you can mine without registering with your ID card or passport, the size of the pool fee (basically the cut that the operator takes for putting everyone together), and the amount of hashrate (the higher the pool's hashrate, the more frequent but small rewards the participants will be getting).

Of course, the mining pools that own a larger piece of the pie can ask for higher fees. But their competition must provide incentives to attract users — so they will lower the fees and also offer extra bonuses such as firmware updates that increase your machine's efficiency and special promotions. In the end, a healthy mining ecosystem will constantly promote competition and prevent centralization. Since its creation in 2011, Litcoin has performed pretty well and there are lots of options from which you can choose for the purpose of maximizing your chances and keeping the largest chunk of the rewards.

	HASHRATE % (02.07.2024)	PAYOUT THRESHOLD	MERGED MINING WITH DOGECOIN	BASED IN	PRIVACY FRIENDLY (NO KYC/AML)	FEE
ViaBTC	24.25%	0.001 LTC	✅	Samoa	✅	4%
F2Pool	20.74%	0.02 LTC/40 DOGE	✅	Cayman Islands	✅	4%
AntPool	18.56%	0.001 LTC	✅	Singapore	✅	3%
Biance Pool	17.22%	N/A	✅	Hong Kong	✅	3%
Litecoinpool.org	6.52%	N/A	✅	N/A, Tor service available a	✅	2%
BTC.com	3.51%	0.001 LTC	✅	"Operated Globally"	✅	4%
Poolin	1.34%	0.01 LTC	✅	China	✅	4%
PowerPool.io	0.909%	0.01 LTC	✅	Spain	✅	1%
Luxor	0.5%	0.001 LTC/100 DOGE	✅	USA	❌	3%
DxPool	0.5%	0.001 LTC/100 DOGE	✅	N/A	✅	3%
Sigmapool.com	1.17%	0.01 LTC	✅	Singapore	✅	1%
Mining Dutch	0.17%	N/A	✅	Netherlands	✅	1%
Zergpool	0.17%	0.05	✅	N/A	✅	0.5%

Last but not least, you should factor in the single most important criterion for determining profitability: electricity cost in your area. Sure, you can become a mining hobbyist and HODL the rewards for years to come just because you can afford to pay the electricity bill. But if you become serious about mining Litecoin, then you will have to make special deals with the electric company or else relocate in places where power is much more affordable.

Proof of Work mining is a race to the bottom in which only the most efficient miners can survive long-term. Naturally, lots of participants can run miners at a loss — but the question is how reliable will their activity be over the years? Nakamoto consensus dictates that miners deal with reward halvings every four years (840.000 blocks in Litecoin). So realistically, there are only two ways to compensate for the 50% split of rewards: either through collecting more fees from participants, or by having the price double every four years. In very extreme cases, users can vote for taxation or even lift the supply cap in order to add the kind of inflation that solves momentary crises but destroys the spirit of a beautiful project.

However, Litecoin's hashrate shows signs of healthy and perpetual growth. Over the last year alone, this metric has grown by more than 25% even if the price action didn't live up to expectations. Which is encouraging and proves that the Litecoin and Dogecoin miners are committed to seeing their favorite projects succeed on the long term. On the other hand, even if the price of LTC and DOGE doesn't increase exponentially, a boost in transaction fees can successfully compensate — so if more people use Litecoin for their purchases, while other use cases such as tokens (Omni-Lite, Ordinals & Runes) and pegged sidechains that pay miners (Drivechains) get enough traction, then the network will remain profitable to mine without significant adjustments.

So if you ever want to use some of the excess energy you produce with solar panels, you have access to fairly accessible energy, or you simply want to support the Litecoin network because you love it, then you have all the information you need to get started.



LOKOTECH

JOIN THE REVOLUTION
DECENTRALIZE THE FUTURE

S1 HASHBLADE
HASHRATE: 2 GH/S
POWER CONSUMPTION: 145W
POWER EFFICIENCY: ~0.0726 J/MH
FORM FACTOR: GPU STYLE HASHBLADE



WORLD'S MOST POWERFUL SCRYPT ASIC MINER
RUN ONE OR STACK MANY

PowerPool.io
Earn More With Ever Hash!

Lokotech.com

Litecoin's MWEB

What it is & how to use it!

MWEB is Litecoin's single most significant breakthrough. It's avant-garde, it's cypherpunk, and it marks a giant leap in the right direction. What it does is to provide an optional privacy and scalability layer that every user can access permissionlessly. It also establishes Litecoin's maturity as a project, as it now dares to diverge from the Bitcoin Core codebase.

Before MWEB, privacy in the context ofBitcoin and Litecoin faced four main criticisms:

1. that adding privacy requires a hard fork that may split the community;
2. that adding privacy diminishes monetary supply audibility and might cause hidden inflation;
3. that privacy protocols cause scalability issues due to increased transaction size;
4. that regulators and centralized exchanges would ban/delist any coin that adds privacy (lol).

MWEB, which stands for MimbleWimble Extension Block, combines two different elements which were once proposed for Bitcoin: the MimbleWimble privacy and data compression protocol, on top of the Extension Block scaling proposal. In order to achieve privacy, coins can now be sent to a parallel private blockchain that's being secured by the same miners. The process of joining this extension block is called "pegging in", while leaving it to return to the base layer is referred to as "pegging out".

How is the extension block different from a merge-mined sidechain? Information about every extension block exists within each Litecoin block. While the sidechain is independent from the main chain, the extension block is an integral part of the design which signals its existence every 2.5 minutes.

Basically, Litecoin is now a combination of the Grin++ and Bitcoin Core codebases, but with an extra scalability layer which allows the main chain to remain transparent. It's also important to mention that this upgrade became possible with a soft fork activation, so it's 100% compatible with older clients that may be lagging or might have technical disagreements with MWEB itself.

Through MWEB, Litecoin acquires the holy grail of sound money qualities: fungibility, which entails that one monetary unit is equal to any other in the same amount. While it's easy to say that 1 BTC equals 1 BTC, you can still discriminate between coins depending on their provenance: money that's linked with the Silk Road, North Korean hackers, or an exchange hack might get rejected by certain economic participants, while freshly-mined coins are usually more desirable. But on Litecoin's MWEB layer, fungibility becomes a reality through a lightweight and scalable implementation of confidential transactions with native CoinJoin mixing functionality and stealth addresses. There is no way to discriminate between MWEB litecoins because the participants can't tell them apart — so everyone has the exact freedom of transactions and benefits from the same amount of confidentiality!

Sure, the privacy in Litecoin's MWEB can't compare with that of a network such as Monero. Opt-in privacy, which is acquired by moving money from a transparent layer to an opaque extension block, has certain limits: for instance, you can know the origin of some main chain funds and track the liquidity that pegs into MWEB. For as long as the coins are being





transacted on the Mimble Wimble layer, they have pretty good privacy and are safe from lurkers. But if the exact same amount (minus transaction fees) gets withdrawn from MWEB to a normal base layer address, then some may assume that the funds belong to the same person.

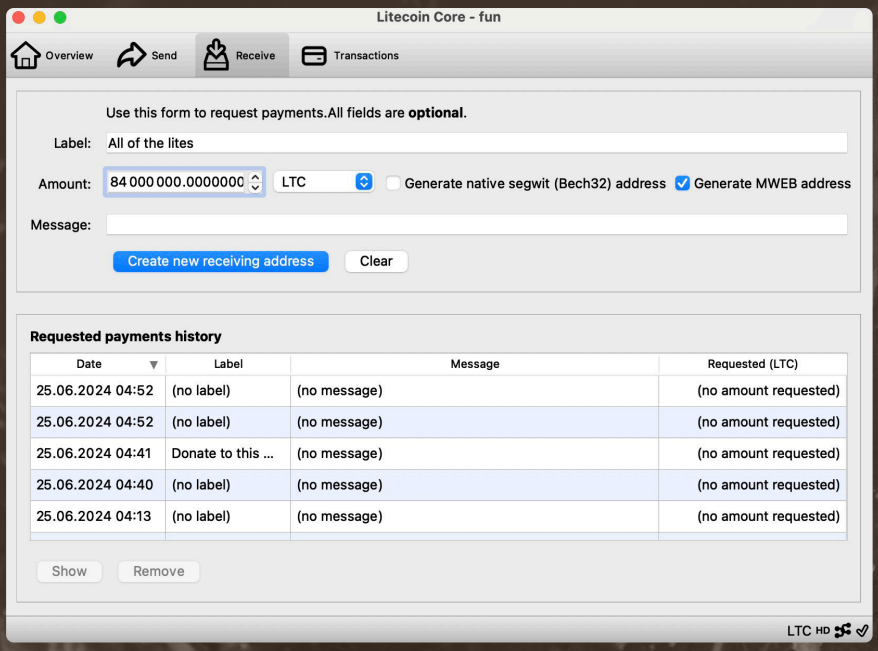
For instance, as of June 25th 2024, the amount of liquidity that's locked into MWEB adds up to 44.2k LTC. If someone pegs in with his 50k LTC and later withdraws 49k to his ltc1 address, then there are legitimate reasons to believe that the same user is behind this transaction. In this particular scenario, the privacy benefits of MWEB are minimal and only relate to the transactions that happen on the extension block. On the other hand, if the user makes multiple daily withdrawals of 200 LTC or less to different addresses, then he/she will have broken the link between the initial peg-in and the later peg-outs within a year. Sometimes privacy is about being indistinguishable from the crowd.

As Charlie Lee explained in S15 E34 of the Bitcoin Takeover podcast, there are 4 dimensions to Bitcoin and Litecoin privacy: network-level privacy, sender privacy, receiver privacy, and amounts privacy. If you run your wallet on Tor or with a VPN, you get network-level privacy — this is only about hiding your IP address from the rest of the P2P network, to avoid linking the activity of your wallet with your geolocation (given by your internet provider). On the other hand, if you generate a new address for every new transaction you're receiving, then you benefit from receiver privacy. In this scenario, based on interactions at the social layer, only the individual senders can know which addresses belong to you.

However, you need technology such as MWEB is order for senders to transact without revealing to the receiver how many coins they have in their wallet. In real life, if you use a $5 bill to pay for a carton of milk that costs $4, then you get your $1 in change and nobody watching this transaction can see what happened in your wallet except for the $5 you take out and that $1 that you put back in. Likewise, tapping your credit card won't reveal to the merchant (and everyone else around you) how much money you have in your account. But if you use Bitcoin or Litecoin without MWEB, any transaction you send will reveal to the receiver how much change came back to your wallet. The UTXO model partially mitigates this issue through coin control, but the MWEB layer completely fixes it. Someone who receives LTC over MWEB will not know how much money the sender might have. The only clue is the amount they received (the assumption being that this sender may have more), but everything else is shrouded in advanced cryptography.

Then there's the issue of hiding amounts for all transactions. Within the MWEB layer, outside observers can only know how many coins are currently locked and might be transacted between participants. Their only clue about what's going on is given by the amounts that come in and out of the extension block. While this isn't as great as Monero (where everything is hidden by default) and Zcash (where this privacy happens on the same layer), it's still a major breakthrough because all of this was possible with a non-disruptive soft fork. Some extra CoinJoins on the base layer (with technology borrowed from open source projects such as Wasabi) can be of tremendous help to boost privacy, as peg ins and peg outs can take place from CoinJoins and into CoinJoins.

Furthermore, if the Drivechain soft fork gets activated on Litecoin, then the Zcash sidechain will provide excellent privacy — and there will be the option to

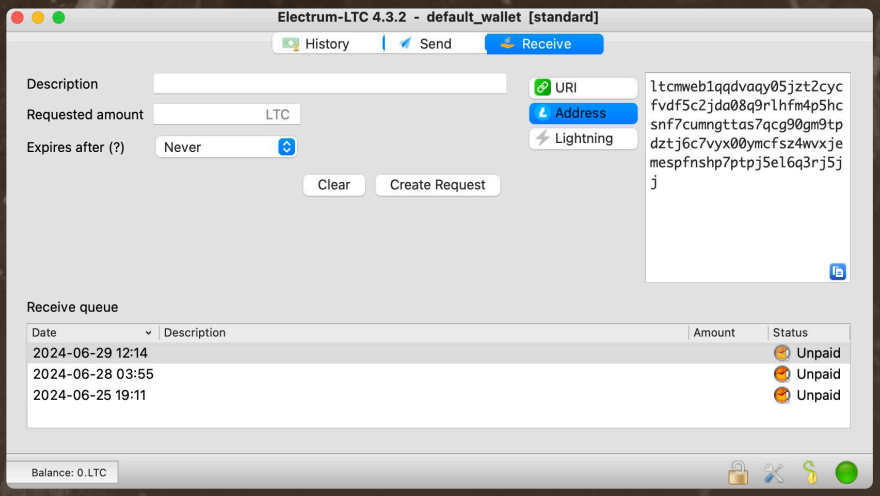


swap LTC from MWEB to ZLite and vice versa. A whole new era of fungibility is upon us, and Litecoin finds itself at the avant-garde of this movement!

Repeat after me: confidential transactions with default CoinJoin mixing features and stealth addresses, on top of an extension block. This is what the MimbleWimble Extension Block is all about!

But wait, there's more: David Burkett, the architect of MWEB, has also made a couple of significant advancements to the MimbleWimble protocol. First and foremost, he figured out a way to enable participants to receive coins without being online while the transaction takes place. This is extremely important, as the user experience is identical with that of Bitcoin and Litecoin. Thanks to this feature, content creators, charities, and fundraising campaigns can just post a QR code or a single address in order to receive coins without having to run a node 24/7. Furthermore, they benefit from great privacy: it's only their business to know how much money they received and they might not even know where it comes from. These people and organizations will only be aware that the particular address that they posted has a designated purpose, so people sent money to it with a particular motivation in mind.

David's second breakthrough was that of making addresses work in the context of the MimbleWimble protocol. By design, MW is not supposed to have receiving addresses. But since this is an integration that's made on top of Litecoin, now we have the ltcmweb address format to complement the user interface.



There's also something to be said about the fact that Bitcoin can simply copy the MWEB design to fix its own issues with privacy and scalability. However, at this time it seems like Bitcoin is mostly focused on enabling a covenant soft fork that can empower devs to build trust-minimized sidechains for lots of different use cases. It's a much more tame approach that probably takes into account the interests of institutional investors and tries to minimize political risk. But it's also a move that makes Litecoin a much more interesting solution for peer to peer electronic cash.

Thanks to MWEB, Litecoin now has its own identity and a value proposition which is very much different from Bitcoin's and Grin's. This middle ground between a transparent base layer and a private extension block might just be the investment thesis that will once again turn Litecoin into a top 10 coin. Once the development is complete and every LTC wallet out there adds MWEB, it's up to the community to use the privacy layer and popularize it through social movements, events, memes, and bullish narratives. Though Litecoin might be the digital silver, fungibility brings it closer to being like gold — a metal that you can melt and cast in different shapes and quantities without any significant material losses.

After this theoretical lesson, let's talk about practical matters: how do you use MWEB? For this tutorial, we're going to use three of the most popular Litecoin wallets: Litecoin Core, Electrum, and LiteWallet. The examples from Litecoin Core are based on version 0.21.3, released on March 29th 2024. Electrum-LTC, on the other hand, received a significant update in June 2024 thanks to the contributions of Hector Chu — now there's a dedicated single-sig setup for MWEB which guarantees that every transaction happens on the privacy-friendly extension block. At the time of writing this article, LiteWallet doesn't have the MWEB integration yet — however, I will be using examples from Newborn: the mobile wallet that's currently being used for testing by LiteWallet developers, and is expected to get merged into LiteWallet sometime in late 2024.

The best way to use MWEB on a desktop computer involves downloading Litecoin Core for your operating system. It's the full node client which unlocks pretty much every feature that's available on the Litecoin network. For more information about the benefits and requirements of running a full node, refer to the dedi-



cated article from this magazine.

Once you've set up Litecoin Core and you're fully synced with the network, go to the "Receive" tab and tick the "Generate MWEB address" box on the right side of the graphic user interface. Write the purpose or destination of this address in the "Label" field, and then click on "Create new receiving address".

Your new address should look like this: *ltcmweb1qqfqfg0rnzlda6plm-4memypplp33cj6lp0kr22j734y3mugnmk-gpvqqe4g3tj8fhdrsm75kyy233u369pzhgr-h6mz79g44w38jdq3nwsfhsss4xuj*

What you have to do next is to send the address you just generated to your friend and wait for confirmations: if your friend is using a normal on-chain address (starting with L, M, or ltc1), then the funds will go through a the peg-in process and you will have to wait for 6 on-chain confirmations (approximately 15 minutes) before the coins become safe to spend. On the other hand, if the transaction comes from another MWEB address, then the transaction is considered final after the first on-chain confirmation occurs in roughly 2.5 minutes.

If you want to peg your own coins from Litecoin Core into MWEB, first go to the "Preferences" option in the menu and pick the "Wallet" tab. Here, make sure you tick the "Enable coin control features" box and restart the Litecoin Core client. Once you're back, go to the "Send" menu and click on the "Inputs..." button on the top-left side of the interface. Here, you will be able to choose which UTXOs (coin stacks from your wallet) you want to send to your MWEB address. For good privacy, don't pick multiple inputs and only peg in one at a time — batching the transaction will only make it more obvious for blockchain analysts that the funds in these addresses belong to the same user and were sent to the MWEB layer at the same time.

In the event that you have your coins elsewhere (Electrum, a mobile wallet, an exchange), the procedure is similar: just paste the correct MWEB address and allow the network to run the process. There might be some wallets which don't recognize the privacy-friendly address format (especially the exchange ones). Don't worry, though: you will just have to make two transactions. One to your full node wallet using a normal ltc1 address, and then a self-transfer from Litecoin Core which pegs your funds into MWEB.

If you own a large UTXO and you only want to peg in with a fraction of your coins, you should also enable the "Custom change address" feature and paste another address from your wallet in the corresponding field. Then go to the "Pay To" field and paste the MWEB address to which you're gonna make the peg-in. Next up, choose the amount you want to send to the privacy-friendly address. As for the transaction fee, 0.0001 LTC per kilobyte (1 litoshi per vbyte) should get you into the next block. Just to be sure, check



the network fees on a blockchain explorer such as explorer.litecoin.net.

The next step is to click "Send", double check that the destination address, the amounts and the fees are correct, and then confirm the broadcasting of your transaction. Keep in mind that these Litecoin transactions are irreversible — unlike Bitcoin, which has RBF to allow you to broadcast the same transaction with a different fee to make it return to your wallet before the first block confirmation, everything is final after you press the "Send" button.

On mobile, the situation is even more simple: all you have to do is to tap on the "Receive" button at the bottom of the user interface and toggle the switch that lets you change the ltc1 address for one that starts with ltcmweb1. If you're going to send your own mainchain coins to MWEB, then copy this newly-generated address and then navigate to the "Send" menu. Here, you will have to paste the address and type the amount that you want to send.

In the version of Newborn (LiteWallet prototype) that I've been testing, there is no option to do coin control (pick which UTXO you want to use for your transaction). But you can use fractions of your balance... and ideally, you should consider moving all the coins that you're willing to spend to MWEB. The privacy benefits are great even if your transactions pegs out of the extension block, as there is no clear record of your coins' provenance.

Interestingly, this MWEB mobile wallet is not entirely SPV — meaning that you don't rely on somebody else's Electrum server, as is usually the case with light clients. Instead, your phone downloads block filters to enable self verification and much better privacy. It's almost as good as a portable personal node, with the added benefit that you can also point the mobile wallet to your own node for the purpose of faster synchronization. With this new approach to mobile wallets, Litecoin is making some serious structural improvements that are worthy of praise.

In Electrum LTC, you can create a new wallet which only generates MWEB addresses. It's great because it's a light wallet (meaning that you don't need to sync a full node) and it works on both Windows and MacOS (with a Linux port on the way). In version 4.3.2, which was developed by Hector Chu and which I was able to test the next day after release, the way to create a new MWEB wallet is to follow this path: "File -> New/Restore -> Name your wallet -> Standard Wallet -> Create a new MWEB seed -> (write down your 12 words) -> (verify your 12 words) -> (set up a passphrase to unlock the wallet file) -> Finally use your wallet!".

The Electrum interface is very simple: you have a "History" tab which shows you all transactions, a "Send" tab that lets you broadcast transactions to any Litecoin user, and a "Receive" tab where you can generate new payment addresses that you can even set up to expire after a certain amount of time. If you're going to transact between your phone and your computer, or you want to recover your LiteWallet funds on your laptop, Electrum is the best way. Unfortunately, Litecoin Core does not support the BIP39 standard to let you recover funds with the seed phrase consisting of 12 words — but Electrum works just fine.

If you want to recover your LiteWallet MWEB funds in Electrum LTC, then follow this path: File -> New/Restore -> Name your wallet -> Standard wallet -> I already have a seed -> (type your 12 words and make sure you make use of the predictive input) -> Click the "Options" button and choose "BIP39 seed" -> MWEB -> Enjoy using your funds on desktop!

At the time of writing this article, MWEB is in the early stages of being integrated into hardware wallets such as Ledger Nano S and Trezor One. There are also rumors that Cake Wallet, the most privacy-friendly multi-coin wallet out there, is planning to support MWEB — which would be super cool, as users could swap LTC for XMR (and vice versa) with great privacy. Most of the groundwork has already been built by MWEB architect David Burkett, Litecoin Core devs such as (Loshan, Hector Chu, and Ultragtx), as well as the LiteWallet team of developers (Kerry Washington, Ivan Ferenčak, Josi Kie, Gean Martinez, and Charlie Lee).

So now that you know what MWEB is and how you can use it, it's time to go to the Moon! Arise, chikun!



LITECOIN and DRIVECHAINS

Drivechains, as described by BIPs 300 and 301, are one of the most radical ways to create monetary maximalism — as defined by the "one coin to rule them all" ideology. Their thesis is simple: put every interesting and useful cryptocurrency idea on a dedicated sidechain, then incentivize the miners to secure them, collect more transaction fees, and serve the users. Though the proposal was made for Bitcoin, it's compatible with Litecoin, Dogecoin, Bitcoin Cash, and every other similar network.



Currently, the legitimacy of new blockchain projects derives from the idea of experimenting with new ideas and use cases. But what if the software, which must get published under free and open source licenses in order to maintain credibility, was copied and implemented on top of a more established blockchain, which issues a cryptocurrency that has a greater network effect (listed on all exchanges, used in commerce, very popular around the world)? Wouldn't this incentivize all the innovation to happen on these sidechains, as developers gradually migrate to the network that pays them in better money, has more users, and gives them better recognition within the industry?

Currently, there are a handful of sidechains that are being developed as part of the Drivechains Launcher initial package. All of them are included in the Drivechain Launcher user interface:

— BitNames: fork of Namecoin, which seeks to decentralize domain names and e-mail;

— BitAssets: layer for porting ERC-20 tokens from Ethereum, as well as ERC-721 NFTs, ICOs, and everything in between;

— Thunder: a big block sidechain with fraud proofs, which has the capacity to process every financial transaction in the world;

— BitEthereum: a 1:1 fork of Ethereum, which enables smart contracts and decentralized applications to get deployed using BTC or LTC as the base currency;

— zSide: a clone of Zcash, which offers privacy by default for all transactions;

— Hivemind: a layer which enables Paul Sztorc to follow his dream of creating a scalable and cost-efficient prediction markets for every interesting event, from sports matches to political elections and everything in between;

If any other idea of use case emerges in the future, it can also get added. But ironically, the entire cryptocurrency industry narrows down to attempts to redesign or refine the concepts above. This means that the entire world of blockchains can get added on top of six sidechains that use only one base currency.

Now let's talk about practical matters: in order to join these Drivechains, users must send their coins into a time-locking mainchain contract that's controlled by miners. What happens next is that the miners take control over the funds and issue the exact same amount on the sidechain that the user wants to use. So let's say that a Litecoin user wants to move 10 LTC to get the best transactional privacy in the industry: he pegs into the zSide sidechain with his coins, then received 10 zLTC in his new wallet. It's the exact same mechanism litecoiners use today for joining MWEB — the most important difference being that pegging out (leaving the Drivechain) can only happen after 3 to 6 months.

In between these peg-ins and peg-outs, users can also perform swaps between chains: let's say that someone has 10 zLTC with really great privacy, but wants to issue shares for a decentralized company on the BitAssets chain — a process which may cost 1 LTC in transaction



fees. The user can perform a swap with someone else who wants to join the privacy-friendly chain, or else pay a service that specializes in trading liquidity across these sidechains.

What keeps the miners honest and prevents them from stealing the coins, you say? Well, there are both incentives and checks and balances. Most importantly, the miners collect transaction fees from every Drivechain that they secure — and according to the specifications of BIP 301, they also join a bidding market for collecting these transaction fees. So they are economic actors whose best financial interest is that the system works. However, if a group of miners refuses to release the funds after the 3-6 months of locking time, then the users can do a soft fork to return the money to the rightful owners. It's an extreme measure, but one which can potentially destroy the reputation of said miners and make them lose their members. Remember, mining pools are just associations of miners from all around the world, which secure the network in a collaborative way and share the rewards between themselves. They can already collude to launch reorg attacks with 51% of hash rate, but the reason why they don't do it is that this will definitely be detrimental for their business model.

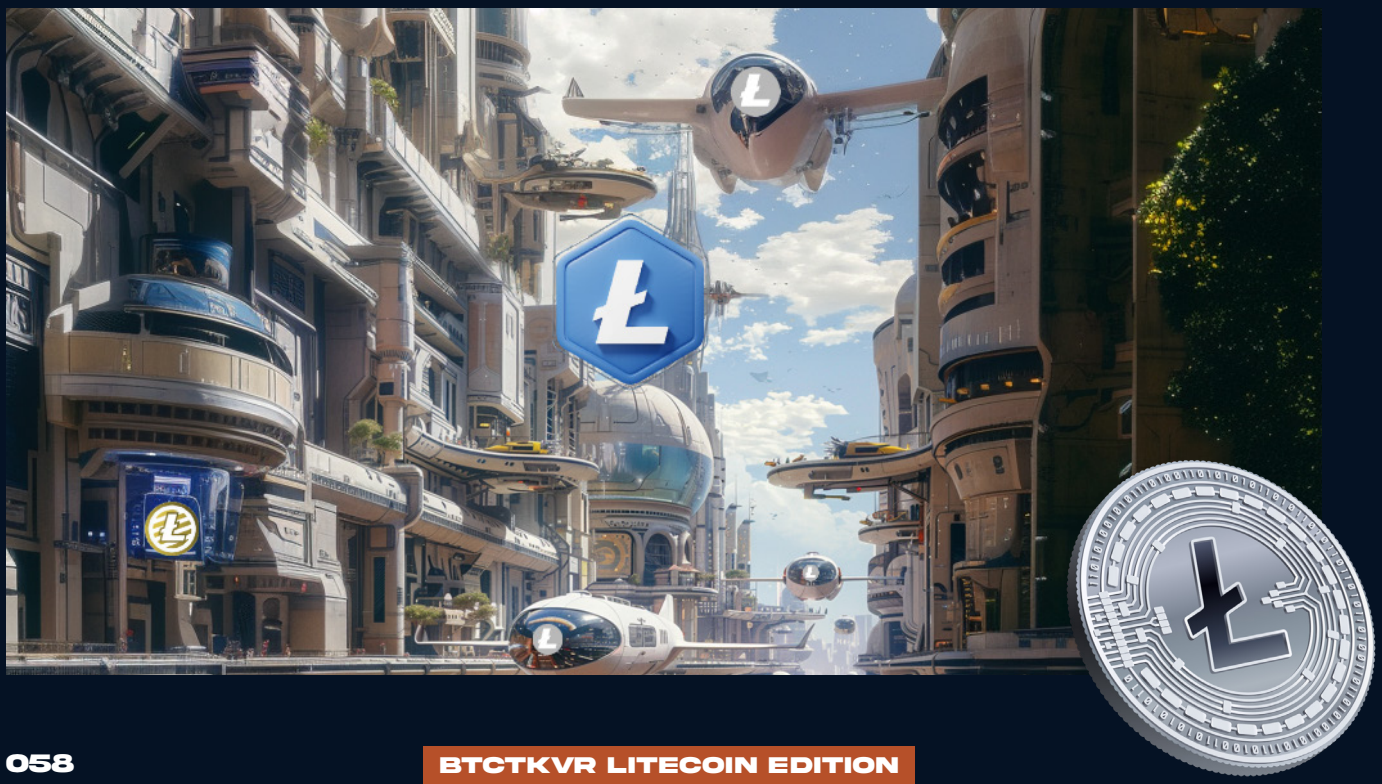
Drivechains are a more advanced implementation of Blockstream's 2015 whitepaper which defines sidechains. Unlike Blockstream's approach, they avoid the lava pit of federated centralization and put the economic actors with most skin in the game (PoW miners) in charge. Drivechains take advantage of the existing infrastructure, maximize mining revenue, and also give the users the features that they desire (privacy, smart contracts, assets, decentralized domain names, fast transactions, prediction markets). As a side effect, this is going to make some layer 1 blockchains redundant: their currency is inferior, they have fewer users, their network effects are small, and the code that gets shipped for them can get copied on Drivechains the next minute. This, in turn, strengthens the currency that implemented Drivechains by maximizing its utility and therefore increasing the market demand for it.

Though they were first proposed on Bitcoin, they didn't reach consensus due to concerns that they might increase mining centralization (for instance, Foundry USA controls roughly 30% of the hash rate under one monolithic company, without third party participants) or else pervert mining incentives (new mechanisms such as voting for decisions and bidding for block rewards did not become very popular). There is another way to activate Drivechains on Bitcoin through a covenant soft fork like OP_CTV or OP_CAT, but this implementation lacks the user protections of BIP301.

If Litecoin activates Drivechains through the BIP 300 and 301 soft forks, attracts developers to work on a superior monetary layer, and gets thousands of new users thanks to the new features, then LTC can even become a threat for Bitcoin itself. In the end, it's the chain that attracts most users and is most resilient to government intervention that wins the race. Litecoin's distribution of hash rate is currently not very concerning, with the top pool ViaBTC only controlling 22%. In the past, the miners have been more than friendly with new ideas: they activated SegWit even when the network didn't really need it, and they also added MWEB without questioning the political risks involved in having a privacy layer. The same miners are also accustomed with merge-mining Dogecoin to maximize their revenue — a move which proved to be essential for their long-term profitability. Based on the track record of Litecoin miners, there is no reason to feel suspicious about their intentions. And then again, any user can mine, set up a pool for others, and effectively dilute everyone's percentage of the hashrate.

For Litecoin, Drivechains can be yet another bold move towards gaining more market share on the crypto market. But ultimately, it's up to the users to create demand for it, advertise it after activation, and convince developers that they should build on top of a superior monetary layer. In the end, one currency is enough to serve 8 billion people. Which one will it be?

integrated merged mining by default: the extended profitability currently pays for the network's security budget.



FAIRLY LAUNCHED ON 13.10.2011. MAKING LITECOIN THE OLDEST ALTCOIN. WITH **ZERO DOWNTIME**, EVER!




BTCTKVR
COORDINATED LUNAR TIME (LTC)
LayerTwo Labs
Bitrefill
LOKOTECH
alephium
LITECOIN FOUNDATION
Lite .Space