CoinShares Research

ASSET HIGHLIGHT: LITECOIN

In addition to its potential as a platform, litecoin has also emerged as an investable crypto-asset. To properly assess the investment potential of this emerging asset, we need context. In the following document we provide said context via: a quick overview of the platform and its component parts; a discussion about current and future growth drivers; an examination of price, volume and transaction trends; a look at litecoin as a portfolio tool; and finally a brief overview of some of the largest risks to the platform.

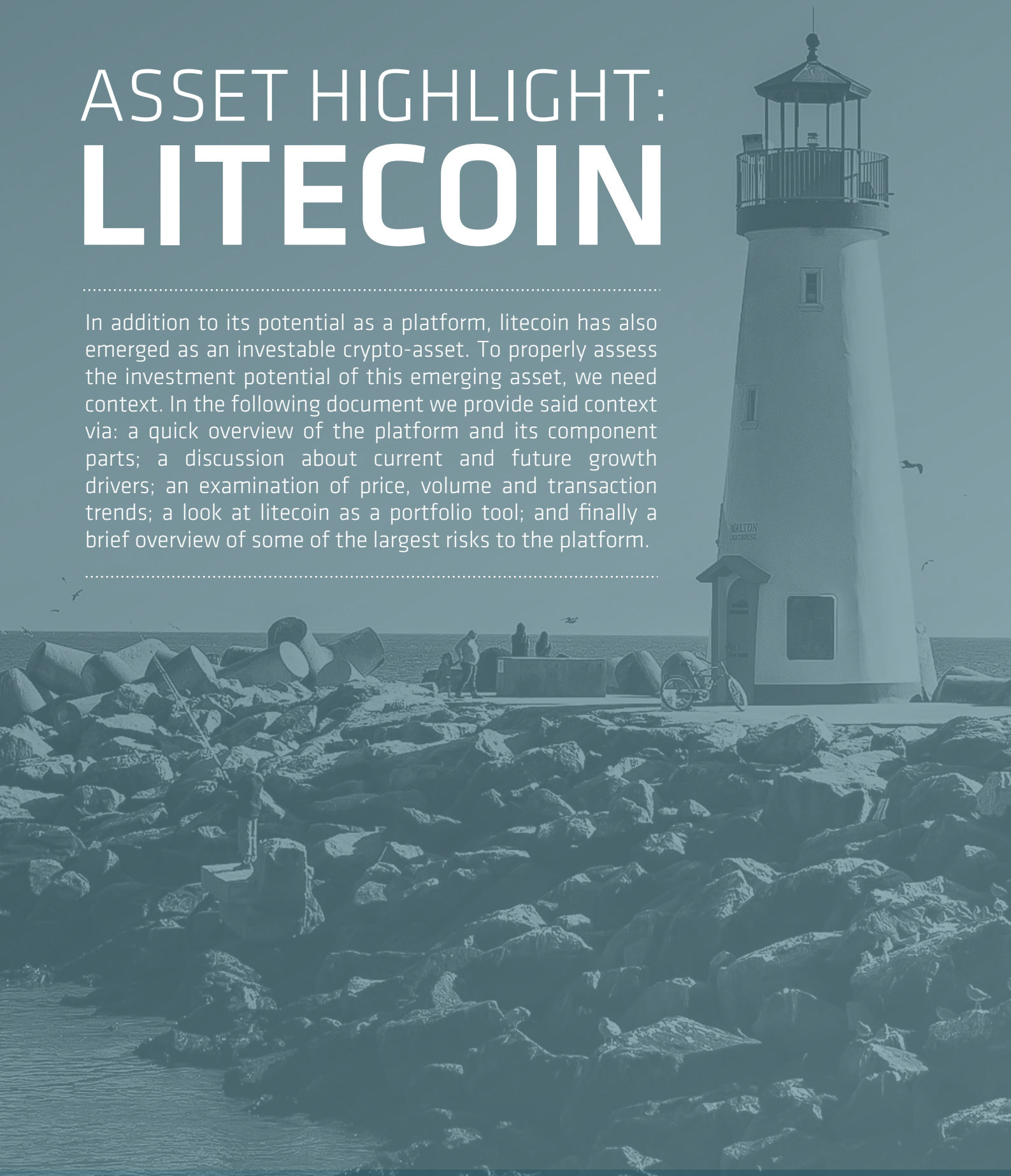


TABLE OF CONTENTS

PLEASE REVIEW THE DISCLAIMER ON PAGE 24

None of the commentary or analysis contained herein is meant to constitute financial advice. This document is meant to be used as a foundational guide to Litecoin and its potential. All analysis is meant to provide emerging trends and observations that may offer value in developing your own investment thesis, though past performance is not indicative of future performance. Please consider all risks carefully prior to making any investment, especially in an evolving asset like litecoin.

LITECOIN BACKGROUND

Litecoin is a true crypto-old-timer with one of the longest running track records of any crypto asset in the market. While most early altcoins suffered from bugs, design failures and lack of community support, Litecoin has maintained a strong, successful record of continuous operation without significant disruption in protocol function.

The origins of Litecoin offer a fascinating peek into the early cryptocurrency mining community and the issues they were facing in the first few years post-Bitcoin. In order to properly understand how the contemporary environment in 2011 facilitated the birth and growth of Litecoin, we need to take a closer look at the state of Bitcoin mining around that time and the community members contributing to the development of the industry.

At the time, Bitcoin mining was fast becoming unprofitable on standard retail computing hardware. Satoshi Nakamoto had originally intended Bitcoin to be mined solely by Central Processing Units (CPUs), the all-purpose processor at the core of retail computers. Unforeseen by Nakamoto however, already by 2010, miners were starting to experiment with modified mining software in order to facilitate bitcoin mining using Graphics Processing Units (GPUs), a class of chips better suited for parallel processing. Successful implementations carried the potential of increasing mining efficiency by orders of magnitude, representing a huge competitive advantage and setting the stage for the creation of highly specialised mining hardware.

While the first known GPU miner is Laszlo Hanyecz (3), of bitcoin pizza fame, the strongest impact on the mining community was arguably made by anonymous mining legend ArtForz. He created highly modified versions of Bitcoin mining software optimised for GPU mining and built some of the first known multi-GPU rigs. While it is impossible to know for sure, BitcoinTalk owner and moderator Theymos estimated that ArtForz' early GPU mining rigs were producing between 20% and 30% of the entire Bitcoin hash rate in late 2010 (4).

Before long, GPU miners were entirely dominating the Bitcoin mining industry and many early miners saw their CPU based miners becoming obsolete and unprofitable. It is this specific mining climate that created the perfect conditions for Litecoin to launch and flourish.

Towards the end of 2011, many miners were looking for alternative ways to monetise their uneconomical mining hardware. This led to the creation of the first Scrypt-mined altcoin, Tenebrix, by Lulcust, using a mining implementation written by none other than ArtForz himself (5).

DEEP DIVE: SCRYPT MINING

Scrypt (pronounced *ess crypt*) is a cryptographic password-based key derivation function originally envisioned for online backup. It is designed specifically to increase the cost of large-scale custom hardware attacks by requiring large amounts of memory in its computation (1).

It takes advantage of the *space-time-trade-off* property of computer science whereby a program or algorithm is subject to an essential trade-off between memory usage and execution time (2).

The idea is to make each computation relatively expensive, e.g. on the order of hundreds of milliseconds, instead of nanoseconds. The effect is that for legitimate human users, who only need to perform the calculation once for authentication, the operation seems near-instantaneous, but for automated brute-force attacks requiring billions of operations, the process would be prohibitively slow and computationally expensive.

With this in mind, it is not hard to imagine how a scrypt mining implementation would be slower to execute *per hash* than a non-memory intensive hash functions such as Bitcoin's SHA-256. In addition, the scrypt memory requirements could initially only be effectively performed by CPUs.

Continued... --->

SCRYPT MINING CONTINUED...

Because of these properties, scrypt mining was meant to re-enable CPU mining and to make the development of Application Specific Integrated Circuits (ASICs) for mining uneconomical. And for a while it succeeded.

However, as the cumulative mining revenue of scrypt-mined coins grew, the potential reward for successful scrypt-ASICs overcame the cost of development, and by spring 2014 the first scrypt-ASICs hit the open market.

Currently, scrypt ASICs have become the industry standard for scrypt mining and specialised mining rigs are now offered by several hardware providers worldwide.

LITECOIN BACKGROUND

Tenebrix rapidly gained popularity by re-enabling CPU mining and tapping into a substantial pool of more or less idle CPUs in the mining community.

Shortly thereafter however, users inspecting the source code discovered that the Tenebrix genesis block contained a coinbase reward of more than 7 million coins, a full third of all Tenebrix ever to be issued. This enormous pre-mine caused outrage in the community and planning soon commenced for a new coin to be forked off the Tenebrix codebase and released fairly in the community. The new coin was to be called Fairbrix and was spearheaded by Charlie Lee (username coblee) (6).

The problem was that Fairbrix was a fork of Tenebrix, itself a fork of Multicoin, itself a fork of Bitcoin, and in that chain of forks, bugs crept in, causing serious protocol issues. In addition to this, neither Tenebrix nor Fairbrix had any caps on issuance, permitting infinite inflation and causing negative reactions in the community. Noticing however, the popularity of the scrypt mining protocol among miners, Lee decided to do a clean new fork from Bitcoin, pick a list of the most promising altcoin features known at the time, and launch it in a fair manner to the community.

The properties chosen were: faster block confirmation times, capped issuance and scrypt mining.

Lee released the Litecoin source code on GitHub 7 October 2011 (7). Two days later, he posted a thread on the BitcoinTalk forum pre-announcing the launch and providing rudimentary Q&A (8). The exact launch time was set to 13 October at 03:00 GMT by popular vote in order to ensure fairness and facilitate maximum immediate participation by the mining community.

The launch proceeded without any major issues and Litecoin went live with a genesis block that included the text: "NY Times 05/Oct/2011 Steve Jobs, Apple's Visionary, Dies at 56".

TECH & ARCHITECTURE

Founders, Governance & Development

Litecoin's principal founder and figurehead, Charlie Lee, has a longstanding history of involvement in the cryptocurrency industry. An alumnus of MIT and Google, Lee made his first post on the BitcoinTalk forum, as coblee, on 27 June 2011 and has remained active ever since.

He worked at exchange provider Coinbase first as engineering manager between July 2013 and July 2015 and then as director of engineering between July 2015 and June 2017. Towards the end of his tenure, Litecoin was listed on GDAX and is now traded there against USD, EUR and BTC.

Lee has a long-standing role as Litecoin lead developer and has expressed his intention of working full-time in that capacity.

The Litecoin reference client is called Litecoin Core and features all "full node" capabilities including complete download and validation of the Litecoin blockchain, all protocol rules and wallet functionality. Most worked projects relate closely to similar projects in Bitcoin and mainly involve safe and proper implementation.

The Litecoin Core website has recently been taken offline, and with it, the full overview of the Litecoin development team. However, before its removal it listed 14 team members as involved with the project.

The Litecoin Foundation serves a political and industrial lobbying function organisationally separate from, but intellectually related to, Litecoin Core. It is a non-profit organisation located in Singapore whose stated mission is to "advance Litecoin for the good of society by developing and promoting state-of-the-art blockchain technologies" (9).

On its board of directors, we find Charlie Lee, Xinxi Wang, Zing Yang and Franklyn Richards. The foundation sponsors two full-time Litecoin developers and also supplies the core team with financial aid on a more general basis.

Generally, Litecoin software upgrades work on the same basis as Bitcoin. Changes can be proposed by anyone, but no user is obliged to install them. Updates are added to the Litecoin Core client based on the meritocratic procedures of the Core development team and all users choose to accept them or not. Like Bitcoin updates, Litecoin client updates are mainly implemented as soft forks and are therefore backwards compatible. This safeguards the networks' decentralisation and robustness by significantly reducing the fragmentation risks associated with hard forks.

In December 2017, Charlie Lee announced that he had completed the sale of all his personal Litecoins with the exception of a small number of physical collectibles. His statement went on to explain that he had taken this action in order to remain detached from the fluctuations of the Litecoin price while continuing his work on protocol development.

While his announcement was interpreted in multiple ways we leave it up to investors to make up their own mind with regards to the potential implications of his divestment on the development of Litecoin.

TECH & ARCHITECTURE

Technology

Like most altcoins, Litecoin was forked from the Bitcoin source code with relatively minor modifications to change a few key attributes. On a technical level, Litecoin is therefore nearly identical to Bitcoin, meaning that pretty much all software upgrades created for Bitcoin can be equally well implemented into Litecoin.

The few actual differences between the two relate mainly to block generation times, coin issuance and the mining algorithm. Litecoin block generation times are targeted at 2.5 minutes instead of the 10-minute block generation target used by Bitcoin. The idea behind the modification was to allow for 4x faster confirmation times than Bitcoin.

Even though the block generation target is 4x that of Bitcoin, the block reward remains the same, starting at LTC 50 per block. However, Litecoin block rewards are cut in half every 840,000 blocks, as opposed to every 210,000 blocks in Bitcoin. As a result, the Litecoin inflation schedule plays out over the same length as Bitcoin (~130 years), but the total number of Litecoins will be 4x that of Bitcoin: a total of LTC ~84MM.

One of the main innovative ideas behind Litecoin was the intention to make mining ASIC resistant to prevent mining centralisation. By employing a memory heavy mining algorithm, the founders were attempting to make Litecoin ASICs uneconomical and therefore retain the possibility of mining on undedicated hardware.

The Scrypt mining algorithm also served a second purpose of being intentionally incompatible with existing Bitcoin mining hardware, thereby ensuring a state of non-competitiveness between the two coins in terms of already operational hash power.

A state of non-competitiveness with Bitcoin is essential for altcoins using the same difficulty adjustment algorithm as Bitcoin. In Bitcoin, the difficulty adjustment algorithm is block-based and therefore asymmetric in the time it takes for it to respond to increases and decreases in hashrate.

In its steady state, Bitcoin will produce one block every 10 minutes on average. The difficulty will readjust every 2016 blocks, which at that rate, is every two weeks. Imagine then for simplicity, that exactly after a difficulty readjustment, the hash rate doubles and remains constant until the next readjustment. It will now only take the network one week to find 2016 blocks, at which time the difficulty would double to accommodate the increase in hash rate. In the meantime, transactions are confirming twice as fast as normal (and incidentally, the coin supply is growing at twice its intended rate).

Let us then consider the opposite scenario: Exactly after a difficulty readjustment, the hash rate halves. The network will now need four weeks in order to find 2016 blocks, at which time the difficulty will be halved. Meanwhile, transactions are twice as slow as normal (and the coin supply, in turn, is growing at half its intended rate).

As we can observe, a doubling in hash rate causes altered network behaviour for one week, whereas a halving of hash rate causes altered network behaviour for one month. Sudden additions of hash power are thus resolved quickly, whereas sudden removals are resolved only after significant periods of time.

This becomes a serious problem for smaller coins with relatively low hash rates that are competing for hash power against larger coins with relatively large hash rates. Because profit-driven miners will migrate between the coins based on momentary profitability, there will always exist a state of flux between the combined hash pools of the coins. For the larger coin, this is not an issue as the hash rate variance is such a small percentage of its overall hash power. For the smaller coin on the other hand, it could be fatal.

Say that their relative hash rates are 1:100. If 9% of miners left the large coin momentarily in search of greater profits, it would represent a 10-fold increase in the small coin's hash rate. This would cause the small coin network to generate blocks ten times as fast for 1.4 days, the difficulty readjusts 10 times upwards. No big deal. The larger coin sees a 9% reduction in block frequency for 16 days. Also, no big deal.

The ratio is now 10:91, and if the same miners migrate back to the larger coin, disaster strikes the small coin. 90% of its miners are now leaving. Transactions are 90% slower to confirm and the network will not find 2016 blocks to readjust the difficulty downwards for approximately five months. Needless to say, an effective network downtime on the order of five months can severely debilitate a coin.

Segregated Witness (SegWit) & Transaction Malleability

Because of its close similarity to Bitcoin, Litecoin has traditionally been extremely quick to implement upgrades intended and written for the Bitcoin protocol, sometimes adopting them before Bitcoin itself. In a sense, Litecoin can therefore be seen as a high-value real-life testnet for new and groundbreaking cryptocurrency technology, and while this does come with a unique set of risks, it also provides the ability for Litecoin to maintain a position at the bleeding edge of cryptocurrency development.

Already by spring 2017, as the first major coin, Litecoin implemented the Segregated Witness (SegWit)

TECH & ARCHITECTURE

transaction structure. This update fixes the transaction malleability bug and thereby opens the door for a whole range of exciting features relying on chained multisignature transactions.

DEEP DIVE: TRANSACTION MALLEABILITY

Transaction malleability is a long-standing issue that has plagued Bitcoin-based coins since it was first reported on BitcoinTalk in 2011.

The problem is caused by the ability of transaction signatures being encoded in different formats -while still containing the same relevant information- being accepted as valid by the network.

A malicious node could then take any transaction broadcast to the network, change the signature -or witness data- format, and publish the alternative but equally valid transaction to the network (it is important to note that the funds will still come from and move to the same addresses, so no money can be lost in the process).

However, this causes a problem because the Transaction ID (TXID) used to reference transactions is a hash of the combined data contained in each transaction, and any minute change to its constituents will completely alter the TXID.

Any applications relying on referencing TXIDs that have not yet been included in the blockchain would be vulnerable to transaction malleability and could not be trusted to safely operate.

One of the most promising features enabled by SegWit is The Lightning Network (see corresponding Deep Dive). First formally proposed by Thaddeus Dryja and Joseph Poon in 2015, the concept would allow for Bitcoin-based cryptocurrencies to scale horizontally -as opposed to the inferior vertical scaling offered by increasing block sizes- by allowing trustless off-chain cryptocurrency payments secured by their underlying protocols. The idea is to run all casual low-value transactions on a second layer network and settle balances using on-chain transactions.

As one of the first protocols to adopt SegWit, Litecoin is supremely placed to benefit from early Lightning implementations. Moreover, due to its close compatibility with Bitcoin, Litecoin's Lightning Network will be fully interoperable with Bitcoin's Lightning Network.

Full interoperability allows for near-frictionless movement of funds between the two blockchains, without the need for a trusted third party. This enables Litecoin to act as an overflow channel whenever Bitcoin

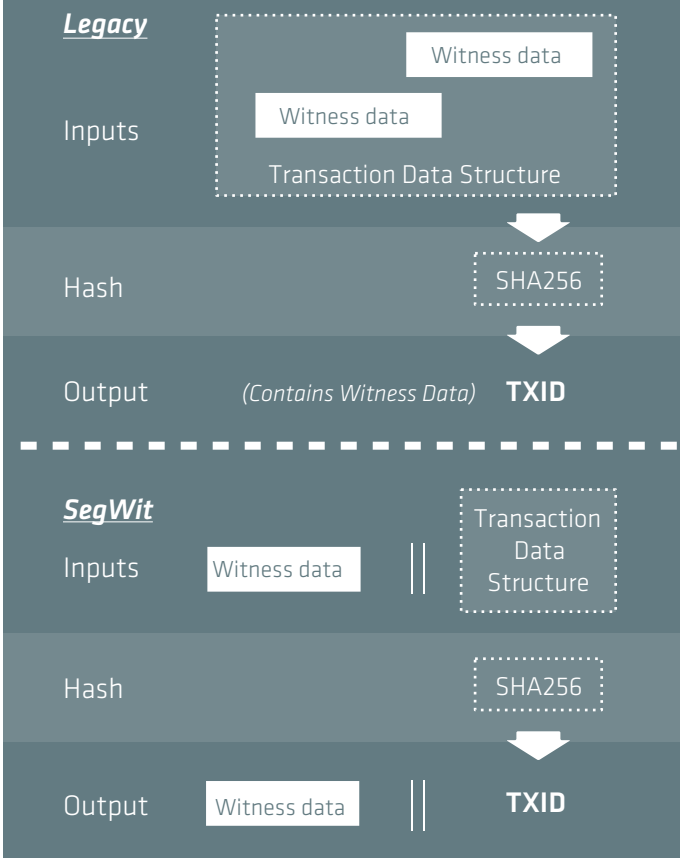
DEEP DIVE: SEGREGATED WITNESS

SegWit is the name commonly used when referring to the Segregated Witness transaction format change first proposed for the Bitcoin protocol as BIP141 in late 2015.

Its primary objective was to solve the transaction malleability issue (see corresponding Deep Dive) thereby facilitating horizontal scaling efforts such as The Lighting Network and new functionality like Atomic Swaps (also see corresponding section and Deep Dive).

SegWit solves the malleability issue by reorganising the transaction data structure. Whereas the legacy protocol includes the digital signatures (the witness data) into the hash input for TXID calculation, SegWit treats it as a separate data structure, not included in the calculation of the TXIDs.

Fig 1. Legacy Structure vs SegWit Structure



Source: Bitcoin.org

By segregating the witness data, calculations of TXIDs are made independently of the signatures, removing the possibility of altering TXIDs by changing the signature formats of published transactions.

Continued... ---->

TECH & ARCHITECTURE

is congested. In this manner, transactions with lower economical value, requiring less security, can be done on the Litecoin blockchain instead, either on-chain or on Litecoin's Lightning Network.

SEGREGATED WITNESS CONTINUED...

During its development, SegWit was further improved to facilitate larger on-chain transaction throughput as well as allow future signature upgrades (e.g. Schnorr) to be implemented without breaking consensus rules and thus necessitating a hard fork.

Under the SegWit structure, block size is replaced by the new concept of block weight. In this manner, SegWit transactions are able to exceed the 1mb block size limit while still operating within the legacy consensus rules. One could say that legacy nodes do not fully understand SegWit transactions, but still consider them valid. Legacy nodes only see the block without the witness data, and therefore considers it to be smaller than the 1mb block size even if, when including the witness, the block is larger than 1mb.

This property is extremely important as it allows an increase of transactional throughput without breaking existing consensus rules which would risk an unwanted network split upon implementation.

As we've already described in our Bitcoin Asset Highlight, there exists an essential trade-off between on-chain transaction capacity and network decentralisation. If all transactions, no matter how trivial were to be recorded in a public blockchain, the system could not support a global number of casual users. For example, 7 billion users doing 2 Bitcoin transactions per day would need approximately 24GB blocks every 10 minutes in a steady state (10). That requires not only a stupendous amount of storage, but also an enviable Internet connection. Both would be extremely expensive and outside of the financial scope of nearly all users. Running a node would be infeasible.

However, small casual transactions do not need strong censorship resistance or trustless, decentralised validation. The economic necessity for censorship resistance is often proportional to the size and importance of a transaction and there is little reason why one would need to store the transactions sent for every single macchiato on a global distributed ledger. The solution is to use the global distributed blockchain as an industrial-grade settlement ledger and do smaller, less economically important transactions on platforms using the immutable blockchains only to settle the final balances.

The Lightning Network

Enter the Lightning Network. Under this system, transactions between counterparties are kept off the blockchain in *payment channels*. On a high level, these payment channels can be thought of as redeemable obligations that either party can settle at any time on the blockchain, even without the trust or cooperation of your counterparty (11) (12).

Payment channels are essentially *state channels*, that is virtual lines of communication through which information is being shared regarding a state. In this case, the state refers to a set of cryptocurrency balances. These states can be updated as rapidly as each party are able to create, sign and transmit transactions to each other over whatever network they are using. Using common internet infrastructure this means thousands of transactions per second for each channel (12).

Channels can be unidirectional (e.g. for metered payments), bidirectional, or multidirectional. They can also be sent in a trustless manner via connecting intermediaries. In the latter instance, and as implemented in the Lightning Network, payments can travel much like routed Internet packets and reach any other user so long as there exists any possible route of open payment channels connecting the two users. For example, if Alice has an open channel with Bob, Bob has one with Carol, and Carol has one with Dave, Alice can pay Dave by using Bob and Carol as payment routing intermediaries.

To initiate a payment channel, two (or more) users send funds to a multisignature address. Both parties provide the other with the signatures needed to close out the channel and refund the initial balance, this way either party can exit the relationship without losses -other than on-chain transaction fees- in case the other party becomes unresponsive or uncooperative.

Any subsequent transaction is kept off-chain, with participants keeping track of the new states of the channel. Each new transaction is structured such that it invalidates or precedes the previous one, thereby retaining at all times the possibility of all participants to close the channel and settle the most recent state onto the underlying blockchain. This prevents both parties from cheating through closing a channel at a previous state not reflecting the latest transactions.

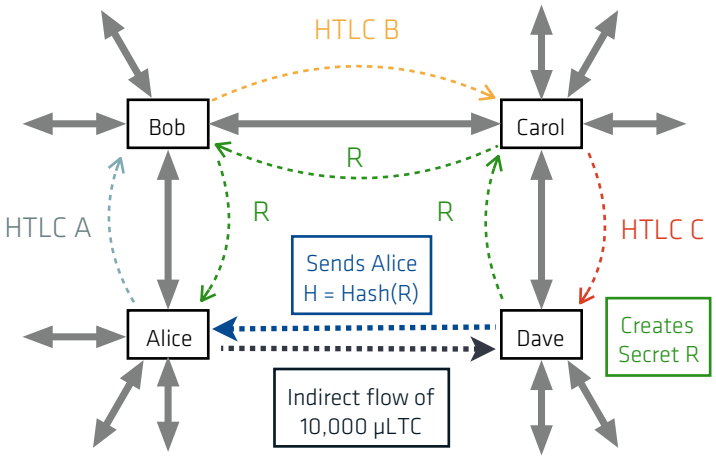
In practice, this is achieved using Hashed Time Lock Contracts (HTLCs, see corresponding Deep Dive), a class of smart contracts running on Litecoin, Bitcoin or any other interoperable protocol. By chaining HTLCs and decrementing the time lock between each channel

TECH & ARCHITECTURE

participant, intermediaries can participate in payment routing without trusting the other participants because they can always pull funds from their preceding counterparty with the same information as their subsequent counterparty must use to pull from them, *before* their preceding counterparty can get a refund. Intermediaries can charge transaction fees as a remuneration for providing their channel liquidity to the routed payment if they so choose.

Figure 2 shows a simplified routing structure between Alice and Dave including simplified pseudo code for the HTLCs. For Alice to pay Dave 10,000 µLTC she first finds a suitable route of open, sufficiently funded channels, in this case via Bob and Carol. She then contacts Dave and asks him to create a secret number R and send her the hash Hash(R) of R. Their contract states that if Alice knows R, she has paid Dave. She can then make an HTLC with Bob such that if he can produce R, which generates H, within (for example) 18 blocks, she will pay him 10,002 µLTC, or else she gets a refund. Bob then makes an HTLC with Carol such that if she can produce R within 12 blocks, he will pay her 10,001 µLTC, or else he gets a refund. Carol then makes an HTLC with Dave such that if he can produce R within 6 blocks, she will pay him 10,000 µLTC, or else she gets a refund. Dave of course knows R and can pull the funds before Carol can claim a refund. Carol then knows R and can pull her funds before Bob can claim a refund. The same holds for Bob and his HTLC with Alice. The 1 µLTC difference in payments represents a transaction fee to entice Bob and Carol to participate in the payment routing.

fig. 2 Simplified Overview of a Routed Payment from Alice to Dave on the Lightning Network



Alice & Dave: If Alice knows R, Alice has Paid Dave
HTLC A: IF R Send 10,002 µLTC, ELSE Refund in 18 Blocks
HTLC B: IF R Send 10,001 µLTC, ELSE Refund in 12 Blocks
HTLC C: IF R Send 10,000 µLTC, ELSE Refund in 6 Blocks
Open Channel

Source: CoinShares Research

DEEP DIVE: HASHED TIME LOCK CONTRACTS

A **Hashed Time Lock Contract (HTLC)** is a technique of conditional payment -a smart contract- in cryptocurrencies utilising Bitcoin's SCRIPT scripting language, that will execute upon the fulfilment of one of two clauses, whichever one happens first.

The first clause is the provision of an input (or proof) that will generate a hash specified in the contract. The second clause is a time marker.

If the correct proof is provided before the time marker is passed the transaction will execute, but if the time marker is passed before such proof is provided, the transaction will refund.

The cryptographic proof of payment received by the payee can subsequently be used to trigger further actions in chained payments, but only if there is no risk of transaction malleability.

HTLCs are essential building blocks of both Atomic Swaps and The Lightning Network.

No participant in the chain can have any knowledge of any other part of the payment chain than the links in which they are themselves involved. This represents a major increase in transaction privacy over regular Litecoin (or Bitcoin) transactions, where all transaction information is published to all network participants.

Only two on-chain transactions are needed for a nearly unlimited amount of Lightning transactions. One to fund the channel, and one to close it. There is no hard lower limit on transaction sizes and fees can be extremely low with no corresponding reduction in security as the system security is effectively piggybacking on that of its parent protocol.

Atomic Swaps

Lastly, we mention cross-chain Atomic Swaps, an exciting cross-currency transaction technique that enables swapping different currencies without counterparty risk. Under the structure of the combined contracts there is no way for one party to receive any funds from the contract unless the other party also gains that same ability. The contracts are also auditable by each party, ensuring that both have the necessary funds to complete the transaction.

Atomic Swaps can be done either on- or off-chain. The on-chain version requires a total of four on-chain transactions, two on each chain, with settlement time and cost depending on the slowest and most expensive underlying chain, respectively. Off-chain swaps can be done via the Lightning Network with all its benefits in terms of speed and cost.

UTILITY & GROWTH OPPORTUNITIES

Sound Money

Litecoin, like Bitcoin owes much of its strength and utility to its independence of authority and censorship resistance. Co-opting a decentralised cryptocurrency against the wishes of its network participants is extremely expensive and nearly impossible to achieve without alerting other stakeholders. The network is relatively simple, but extremely robust.

Litecoin as a currency is impossible to debase without the express consent of a majority of the network. A system, not relying on any level of trust whatsoever and whose only assumption is that every participant on average acts in their own perceived self-interest: the very foundation on which modern economic theory already rests.

Most Valuable Use Cases

At present, we hold that there are three main high-level use cases dominating Litecoin utilisation which comprise its value. The three are, in no specific order of prevalence 1) medium of exchange, 2) store of value, and 3) instrument of speculation. We will discuss its role as a store of value and instrument of speculation later in this section.

Medium of Exchange

Out of the three main high-level use cases, specific subsets emerge. While this paper cannot cover them all in detail, we will concentrate on two particularly promising ones emerging from its utility as a medium of exchange: payments and settlement.

Payments is one of the more obvious applications for borderless, permissionless value transfer protocols. Money can be transmitted anywhere in the world where there is access to electricity and the Internet, with flat fees regardless of amount transferred. A Litecoin transaction will cost the same whether you are sending LTC 0.001 or LTC 10,000. Furthermore, Litecoin's increased block frequency compared to Bitcoin lends itself better towards payments as transactions clear securely (6 confirmations) in an average of 15 minutes as opposed to an hour for Bitcoin.

However, as we have previously discussed, the pure utility of using the protocol layer for direct payments carries with it an essential trade-off between scalability and decentralisation, such that under current protocol rules and network architecture, "on-chain" payments at global scales are not feasible.

This limitation takes us straight into the realm of the settlements use case via the Lightning Network. Because it makes little to no economic sense to enter every single transaction into a global distributed blockchain, a more suitable role for 'protocol layer transactions' is settlement. If all parties to any aggregation of payments, agree on the final balance, settlement on a permanent, immutable, indisputable ledger represents a much more economically sound alternative to storing every transaction, no matter how small, directly on-chain.

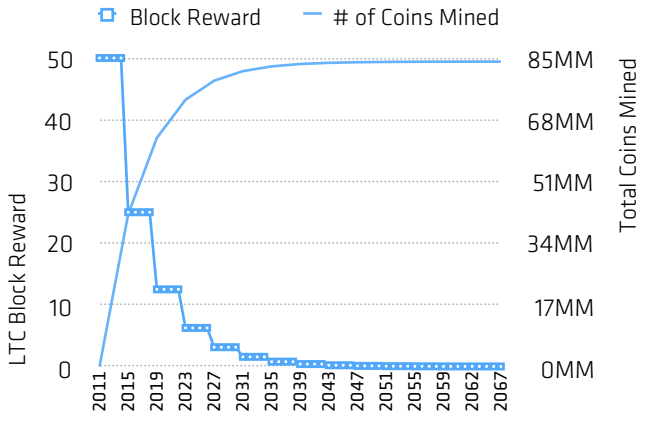
Solutions using the Litecoin network as an underlying mechanism for clearing or settlement are referred to as Layer 2 (L2) solutions. While there already exist centralised payments solutions available for merchants seeking to accept litecoin payments, these still suffer from the same legacy issues as trust-based payments, without being able to fully capitalise on the trustless decentralised properties of Litecoin.

Store of Value

Litecoin is envisioned as the digital silver to Bitcoin's digital gold. As touched on in the Technology section, litecoin issuance is capped with an upper limit of LTC 84MM and no more can ever exist, this is analogous to the finite supply of precious metals in the earth's crust.

Emission is periodically constant against an increasing money supply and halved approximately every four years. From its initial coinbase (the technical term, not the company) reward of LTC 50 per block, the block reward has since been reduced to LTC 25 in 2015. Annual Litecoin inflation will still remain above 9% until dropping to around 4% at the next halving projected in 2019, and then less than 2% at the subsequent halving, around 2023 (Fig. 3). At some point, however, Litecoin will turn deflationary. Because it is possible to lose private keys or send litecoins to unspendable addresses, litecoin issuance will eventually be outpaced by litecoin losses, ultimately reducing the spendable supply.

fig. 3 Time Series Projection of Litecoin Block Reward (LTC) Versus Total Coins Mined



Source: CoinShares Research

SPECULATIVE VALUE & RELATIONSHIPS TO WATCH

In this section we have mapped some possible drivers of growth in the utility value of the underlying Litecoin network. These are nonetheless single components in the aggregate price and thus affects network value in a non-exhaustive manner. The section bears close resemblance to its sister sections in our Bitcoin and Ether Asset Highlights since many of the relationships highlighted are equally interesting for most cryptocurrencies.

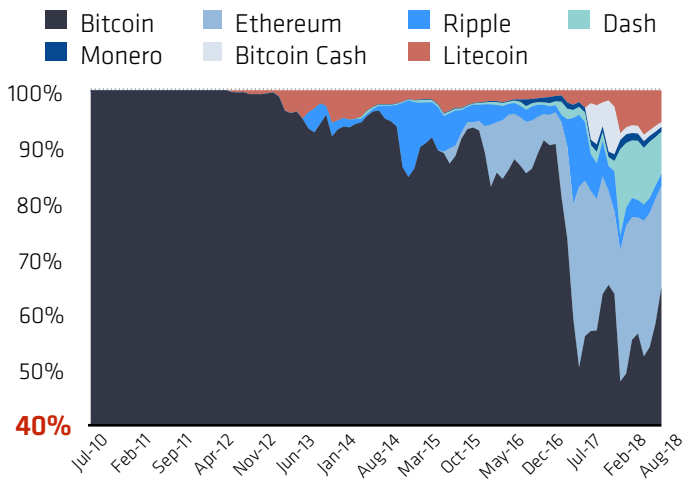
Speculation plays a substantial role in driving the litecoin price and this speculation is influenced heavily by the performance of other cryptocurrencies and the market as a whole. There are many other decentralised tokens with which litecoin competes on both technical and speculative fronts and their relative performance over time has an impact on speculative belief. One trend to watch when evaluating performance is the overall dominance (share of the decentralised token market's outstanding value) of litecoin among its closest competitors.

Dominance

We measure dominance among crypto assets as the percentage of cumulative network value (modelled on conventional market capitalisation). Since its first publicly-priced trades, litecoin has seen its unit value rise from a few cents to a peak of more than $400. Even in the face of widespread new competition, litecoin has steadily remained among the top 5 crypto assets (Fig. 4)

But more than merely measuring each currency's relative valuation/standing, the long-term dynamics of the dominance curve can illuminate trends in funding patterns between competing protocol technologies. As systems develop, each addition or reduction of value to the codebase should elicit organic responses in the volume and momentum of funding flows between coins as investors re-weight their holdings based on their belief in the viability of the technologies.

fig. 4 Cryptocurrency Dominance as Percentage of Combined Market Cap Since Bitcoin Launch

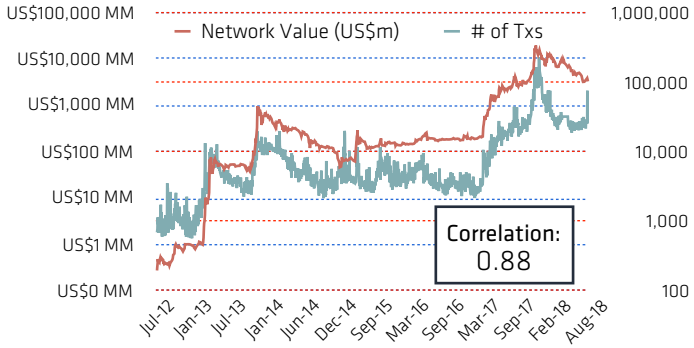


Sources: bitinfocharts.com, CoinShares Research

Transaction Volume

Speculative value in litecoin is part-driven by future expectation of utility, weighted (or inflated) by current level of hype. One indicator many digital asset speculators watch as a relational indicator of both price and network value is the development of daily on-chain transaction volume as a proxy for adoption and growth in usage. We observe a very strong correlation between daily on-chain litecoin transaction volume and network value (Fig. 5).

fig. 5 Network Value Versus Daily Litecoin On-Chain Transaction Volume (# of Transactions)



Sources: bitinfocharts.com, CoinShares Research

Exchange Volume

We also observe a strong correlation between exchange traded volume (US$) and Litecoin network value (Fig. 6, next page). However, because exchange volume ($) and network value ($) both contain the litecoin price as components of their calculation, this may create an inflated sense of covariance between the two.

To standardise the relationship, one can look at litecoin-denominated exchange traded volumes. These have grown since inception, an impressive statistic given the meteoric rise of the litecoin price. This relationship does, however, correlate much less strongly than dollar denominated volumes versus network value (Fig. 7, next page).

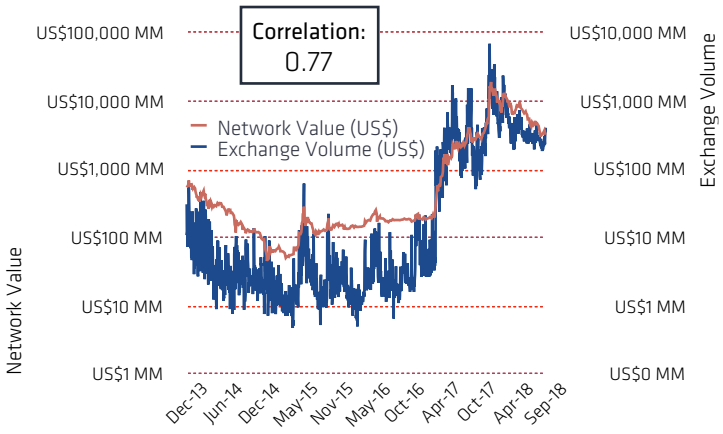
Although trade volumes are valuable data points when analysing bitcoin price trends, there are some attributes of various crypto-exchanges that should be noted with caution when looking at available data.

SPECULATIVE VALUE & RELATIONSHIPS TO WATCH

There has been, and to a certain degree remains, a tendency for upstart exchanges to offer zero, or token-subsidised trading fees in order to attract traders. While this is the complete prerogative of each individual exchange, one consequence of zero-fee trading is that volumes may appear stronger than what could be reasonably expected at more established exchanges where fees are levied.

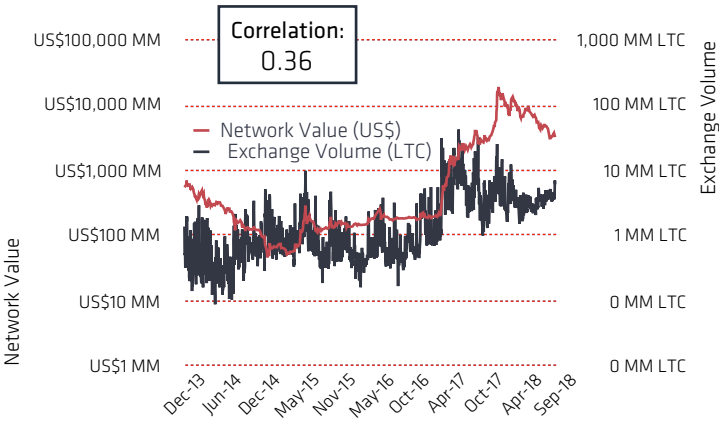
Our exchange volumes do not include exchanges with zero or token-subsidised fee structures.

fig. 6 NETWORK VALUE VS. US$ EXCHANGE VOLUME



Sources: Coinmarketcap.com, bitinfocharts.com, CoinShares Research

fig. 7 NETWORK VALUE VS. LTC EXCHANGE VOLUME

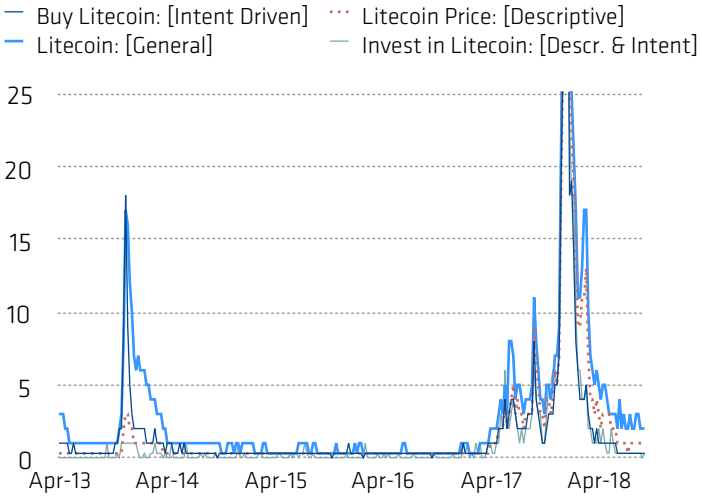


Sources: Coinmarketcap.com, bitinfocharts.com, CoinShares Research

Search Trends

Five-year Litecoin search trends reveal strongly hype-driven cyclical interest spikes of increasing magnitude (Fig. 8). Temporally, the peaks are narrow and correlate closely with historical spikes in litecoin price and the corresponding media coverage. Overall this suggests a market that has thus far been reactive to cyclical speculation on future utility value.

fig. 8 GOOGLE SEARCH TRENDS FOR LITECOIN TERMS



Source: Google Search Trends

It is worth noting that these volumes are indexed against the top values and therefore look very subdued in comparison to the peak-hype volumes. We have therefore cut the axis at 25% of the peaks to better show the long term trends.

Even though the baseline search volumes are somewhat drowned out by the sheer magnitude of the spikes, they do reveal a slow but steady increase in long-term search interest. Current general litecoin interest is roughly a quarter that of the same time last year, but more than three times that of two years ago.

ASSET PERFORMANCE & CORRELATIONS

As is the case with many crypto assets, measuring pure asset returns over the entire lifetime of litecoin will return figures that verge on the absurd. Litecoin, like bitcoin, was not pre-mined and started its life priced at US$ 0 (even though its cost of creation has always been higher than US$ 0). Therefore, its return to date is technically infinity, which does not make for good comparisons. If we instead begin in 2012, when decent price signals for litecoin had been established, we can begin to look at returns in numbers that are at least closer to the orders of magnitude we are used to.

SPECULATIVE VALUE & RELATIONSHIPS TO WATCH

Table No.1	2012	2013	2014	2015	2016	2017	2018 (YTD)
Returns	117%	33539%	-89%	30%	25%	5049%	-71%
Volatility	35%	147%	85%	88%	36%	112%	78%

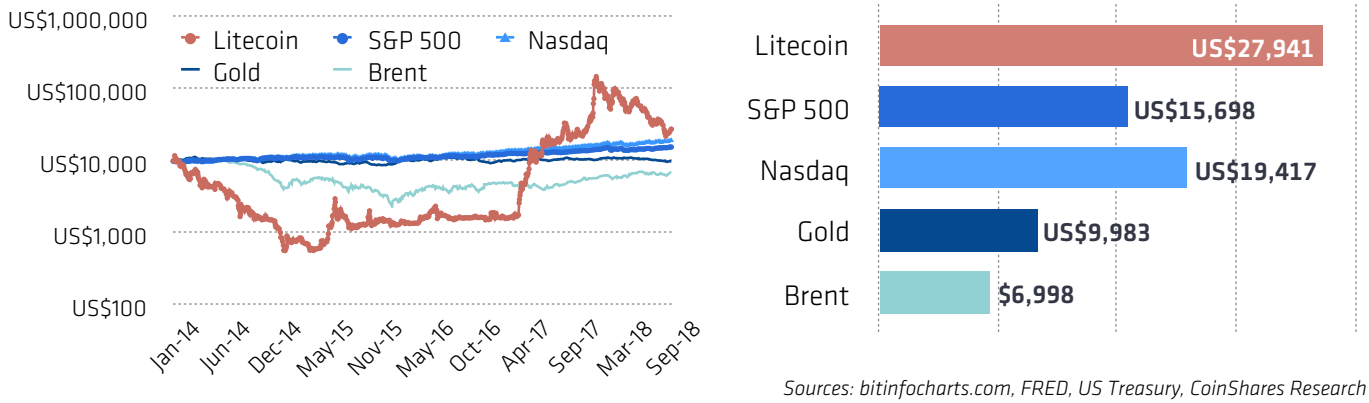
Sources: bitinfocharts.com, CoinShares Research

Investment Case of US$ 10,000

As a relative comparison it can be helpful to index a potential set of portfolio components to see how they perform in relation to each other. In this case, the index would start each asset with a US$ 10,000 investment at the end of 2014. For comparison - we've chosen a basket of commonly invested assets (S&P 500, Nasdaq Composite, Gold and Brent), versus the performance of litecoin.

What we see is that litecoin was the worst performing investment until mid-2017, at which point it raced past every single other asset, twice surpassing $100,000 before correecting through much of 2018. As of the last data point (02 September 2018), that US$ 10,000 investment, if made at the end of 2014 would be worth approximately US$ 28,000.

fig. 9 DEVELOPMENT OF US$ 10,000 INVESTED IN COMMON INVESTABLE ASSETS 2014 TO 2018 (YTD)



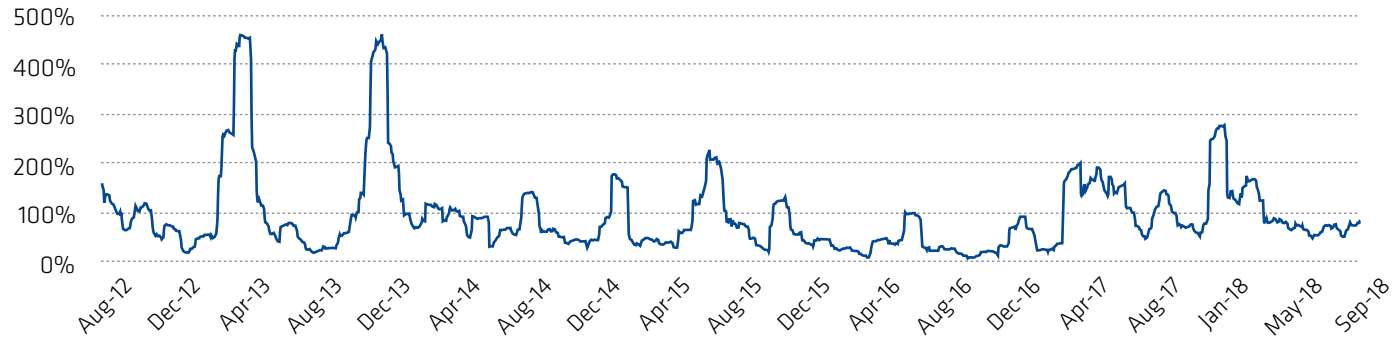
Sources: bitinfocharts.com, FRED, US Treasury, CoinShares Research

Volatility

However, in order to access returns on these levels, litecoin investors must withstand severe volatility.

Looking at historical annualised figures for litecoin, we observe that the multi-year trend of falling volatility was broken last year as hefty price action yet again caused large fluctuations in prices (Fig. 10). While we suspect volatility might dampen over time as the price reaches maturity, litecoin still behaves like a growth asset requiring substantial risk tolerance on the part of investors.

fig. 10 LITECOIN VOLATILITY 2012 - 2018 (YEAR-TO-DATE)
(30-DAY ROLLING ANNUALISED STANDARD DEVIATION OF DAILY RETURNS)



Sources: bitinfocharts.com, CoinShares Research

ASSET PERFORMANCE & CORRELATIONS

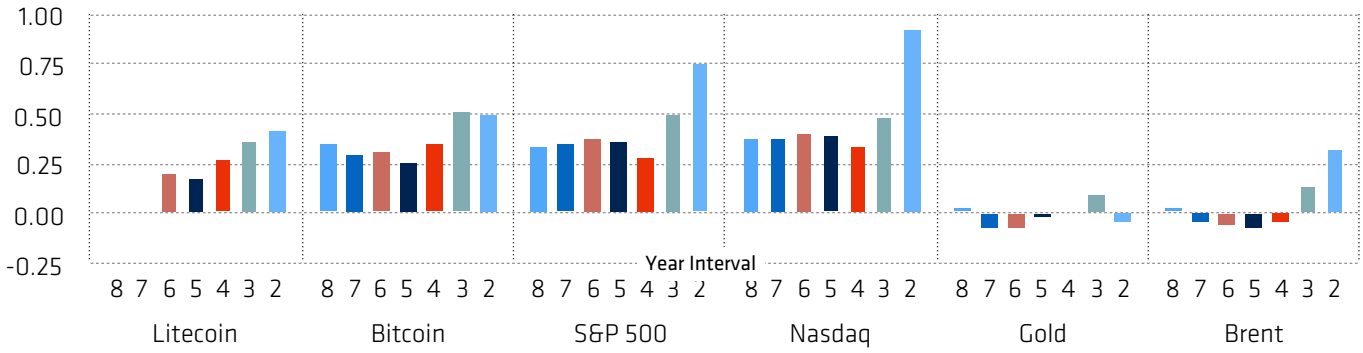
Risk-Adjusted Returns

Neither pure returns nor volatility alone suffice as metrics for prudent portfolio allocation. Because assets are inherently different and incorporate unique risks, returns and volatilities, one must also look to risk-adjusted measures in order to achieve a valuable comparison.

Sharpe Ratios offer one method of comparing returns on the basis of standardised volatility measures. First, pure returns are discounted by a risk-free investment rate, represented by 3-month U.S. Treasury bills. Average excess returns above the risk-free rate are then divided by the price volatility of the asset, represented by the standard deviation of the excess returns. Assets with the highest Sharpe Ratio offer the best compensation to investors for the level of risk they are taking.

Litecoin is an extremely volatile investment asset. Even so, when applying the Sharpe Ratio to litecoin and a basket of commonly investable assets, litecoin scores moderately well against stock indexes like the Nasdaq and S&P 500 while consistently beating commodities like gold and oil (Fig. 11).

fig. 11 (8-2YR) SHARPE RATIOS - MONTHLY RETURNS (VS. 3-M US TREASURY BILL) OF COMMON ASSETS



Sources: bitinfocharts.com, FRED, US Treasury, CoinShares Research

Returns Compared to Common Assets

One of the most exciting attributes of the cryptocurrency space is highlighted in Table No. 1 (Page 12): Whereas assets with similar returns (and risks) have largely been unavailable to anyone outside the venture capital industry, the open nature of crypto-markets has made high-risk/ high-return assets accessible to a much wider public. The 3-month returns in Table No. 2 makes the risk/reward relationship of the crypto-space compared with more 'traditional' assets abundantly clear.

Table No.2	Litecoin	Bitcoin	S&P 500	Nasdaq	Gold	Brent
Q3 2016	-9%	-9%	3%	9%	-1%	1%
Q4 2016	14%	**59%**	3%	1%	**-13%**	**14%**
Q1 2017	**62%**	12%	6%	**10%**	9%	-5%
Q2 2017	**443%**	**126%**	3%	4%	0%	**-10%**
Q3 2017	**41%**	**77%**	4%	6%	3%	**21%**
Q4 2017	**315%**	**213%**	6%	6%	1%	**17%**
Q1 2018	**-49%**	**-50%**	-1%	2%	3%	3%
Q2 2018	**-30%**	-6%	3%	6%	-6%	**12%**

Sources: bitinfocharts.com, FRED, CoinShares Research

ASSET PERFORMANCE & CORRELATIONS

Correlations of Returns per Asset

Extending the discussion on comparative returns, Table No. 3 (below) shows the 2-year correlations between the daily returns of litecoin (since 2015) against the same set of assets as in Table No. 2 above, using Pearson's Correlation Coefficient.

The inclusion of uncorrelated assets into a diversified asset portfolio generally serves to lower its overall volatility. Thus, large movements in single assets only affect the overall portfolio value in a dampened manner as the probability of all assets moving together is low. Conversely, if all portfolio components move in unison there is an increased propensity for the entire portfolio value to follow the movement of single assets and greatly diminishing diversification benefits.

The daily returns correlation between litecoin and traditional investment metrics such as the S&P 500, Nasdaq, Brent Crude and Investment Gold indexes is nearly zero. This property makes litecoin uniquely interesting as a portfolio-balancing tool for investors seeking diversified exposure to multiple assets.

Table No.3 — 2-Year Correlations of Daily Returns

	Litecoin	Bitcoin	S&P 500	Nasdaq	Gold	Brent
Litecoin		0.61	-0.0034	-0.020	0.033	0.0021
Bitcoin	0.61		-0.027	-0.038	0.055	0.004
S&P 500	-0.0034	-0.027		0.94	-0.091	0.25
Nasdaq	-0.020	-0.038	0.94		-0.081	0.17
Gold	0.033	0.055	-0.091	-0.081		0.0018
Brent	0.0021	0.004	0.25	0.17	0.0018	

Sources: bitinfocharts.com, FRED, CoinShares Research

RISKS

Major risks to Litecoin can be roughly classified into three general categories: Technological risk, and attack/regulatory vulnerability, with certain cases of overlap. Here we will outline the most pressing risks, as we see them, with the express caveat that we cannot possibly cover every conceivable one.

Key Personnel Risk

Litecoin, like Ethereum, has a well-recognised leader and figurehead whose persona acts as the ultimate decision authority in matters relating to vision and development. Litecoin is therefore vulnerable to the wellbeing, continued motivation and productivity of its founder and leader, Charlie Lee. If any detrimental event or series of developments should befall Mr. Lee, there are significant risks of disruption to both the development team and the Litecoin Foundation.

Such disruption can range from power vacuums and infighting as current stakeholders vie for power over the future of the protocol to simple disagreements on protocol changes going unresolved for extended periods of time, potentially even leading to political chain splits.

Block Reward Tapering

Mining rewards have two current constituents: the block reward and the transaction fees. Sometime around the year 2140, the block reward will round to zero, ending the fresh issuance of litecoins. However, because of the shape of the issuance curve (see Fig. 3), approximately two thirds of all litecoins have already been issued, and before 2040, this figure is expected to be 99%.

At current litecoin prices the cumulative annual block reward is worth almost US$150MM. The total value of the block reward plus transaction fees is what makes an attack on block consensus prohibitively costly, preventing certain malicious behaviours in the consensus layer. For these types of attacks to remain unreasonably expensive to execute, either total transaction fees must grow to replace the block reward,

RISKS

or the litecoin price must rise in an inversely proportional manner to the block reward, or the more likely scenario, there must be a combination of both.

For a dependable fee market to develop, there must be a balance between transaction throughput and transaction fees. Economists will swiftly point out that equilibrium will arise between transaction costs and transaction throughput, determined by transaction supply and transaction demand.

But for a price to exist the quantity of a good cannot be unlimited, and so there must at all times exist some restriction on the availability of block space (this, in return, causes other potential issues which we will cover further in the next section).

Finding the correct balance between restricting block space and allowing sufficient throughput to cover demand is not a trivial matter and no commonly accepted solution has yet been offered. Unless a reliable stream of transaction fees can be expected to incentivise mining, Litecoin's consensus security model risks collapsing with potentially devastating consequences for investors.

Scaling

Cryptocurrency scaling is a highly complex problem that cannot be sufficiently covered in the scope of this paper. We will endeavour to give a surface-level overview of the problems that has received the most publicity but would like to stress that the matter is much more complicated than it first appears. For a more thorough treatment of Bitcoin scaling (which applies equally to Litecoin) we can refer you to the Bitcoin Wiki (13) and the Bitcoin Core Capacity Increase FAQ (14), and we recommend a detailed investigation of their listed sources.

Under the current protocol, Litecoin transactions are limited to approximately 28 per second (13) (15), depending on the size and type of the transactions. Litecoin, like Bitcoin has a blocksize limit of 1 megabyte, assigned as a spam-reduction measure to reduce blockchain bloat, but due to the increased block frequency, Litecoin can handle four times the transaction load of Bitcoin.

As we keep repeating, there exists an essential trade-off between on-chain transaction capacity and decentralisation. There are two reasons for this, but both relate to the cost of operating Litecoin nodes, affecting the number of network participants who could afford running a full node.

The first reason is cost of storage and validation: All full Litecoin nodes must validate all transactions and keep a full copy of the blockchain in order to verify transaction history back to the genesis block.

If every single transaction of a payments network on the scale of Visa (on the order of 5,000 per second (16)) were to be recorded in the blockchain, it would grow by more than a hundred gigabytes per day (13), making it unrealistically expensive for most people to run a node.

The second reason is slightly more complex and results from bandwidth limitations: In our Ethereum Asset Highlight we briefly touched on the concept of stale or orphaned blocks. A stale block is a valid block found by a miner that reaches the network too late because another miner has successfully propagated a different valid block to the network. Unlike the Ethereum protocol which rewards stale blocks as Uncles, stale blocks in Litecoin are simply disregarded by the other nodes and the cost borne by the orphaned miner.

If we assume an average Litecoin transaction size of 500 bytes and a peak transaction demand of 5,000 per second, each 2.5-minute block would need to contain approximately 125 megabytes of data (13) (15). Acknowledging that not all locations currently have access to high-speed Internet connections, transmitting such a large block reliably to the entire network could take several minutes.

This would greatly increase the chances that another miner finds a valid block and successfully propagates it, before your own block is sufficiently propagated, risking that it becomes stale. Such an effect has a particularly centralising pressure on mining as co-located miners would benefit greatly from reduced transmission times between each other.

Additionally, as we mention in the previous section, the supply of a good must be limited for a price to exist. This creates a friction between increasing block space for scaling purposes and limiting it for the sake of securing sufficient fees to cover future mining rewards. The balance between the two is perhaps one of the most hotly debated topics in the Litecoin and Bitcoin communities and one that largely remains unsolved from a community consensus standpoint.

It is important to realise that scaling Litecoin by multiple orders of magnitude is not impossible; it just simply cannot be done under the current protocol structure. However, the immaturity of the current software and the need for significant upgrades to the protocol in order for Litecoin to compete as a value transfer network on a global scale represents a notable risk to investors.

Harmful Legal or Regulatory Action

Although Litecoin, like any other distributed network, cannot effectively be shut down without finding and disabling almost every single network participant, it is still vulnerable to damage dealt to it by powerful state

RISKS

actors. Damage of this kind cannot realistically kill the network, but it can certainly inflict severe monetary loss on network participants and deal powerful blows to adoption and use.

While, for example, outlawing the software is entirely unenforceable, it would almost certainly drive many participants off the network for fear of government repercussions, causing negative price pressures. Overly burdensome regulation can have much of the same effect.

With the notable exception of a handful of undemocratic countries, state-level responses to most cryptocurrencies have thus far been measured and reasonable. Most governments have chosen to observe its growth and development, more or less leaving it alone so as to not stifle innovation. This is a very reasonable response to an ecosystem, whose total network value has until recently been lower than most Fortune 500 companies, however, we cannot assume this cautious approach will continue as the total network value of cryptocurrencies begins to approach the M1 value of major world currencies.

Running a Full Node is Costly and Technically Challenging for Most Users

Unlike mining nodes, regular full nodes are not directly compensated for their services by the network. Running a full node is in the self-interest of litecoin holders as it is the only way users can be certain that none of the protocol rules have been broken by other participants without relying on someone else's trusted information.

However, operating a node comes with a very real cost and normally requires separately dedicated hardware on the part of the user. Although there is specialised lower-cost hardware coming to market it is still expensive enough that only a subset of all users can be reasonably expected to have a separate computer running Litecoin Core. There are less hardware intensive ways of running a full node, but these solutions, while not immensely technically challenging, are still sufficiently difficult to put off most casual users.

Competition & Technological Obsolescence

Since the first altcoins began emerging a few years after Bitcoin's invention there has been a Cambrian explosion of new coins and tokens in the cryptocurrency space. Altcoins now number in the thousands, and with the rapid proliferation of ERC-20 tokens, this trend has only accelerated. There is a chance that a newer alternative coin could outcompete Litecoin.

Hostile State-Level Adversaries

State-Level actors could choose to covertly attempt to harm the Litecoin network. It is not difficult to imagine how branches of government stakeholders in the current financial system could come to view cryptocurrency as a threat and choose to take aggressive action.

Such an effort, especially one not overtly giving away their hostile intent, is likely to be directed at the community itself. Because Litecoin's architecture is robust in the face of outside attacks, the most effective assaults might have to come from within. A classical method for such a strategy is to foment internal hostility within the community, creating factions, which will expend considerable time and energy on infighting while leaving the overall network fragmented and more vulnerable to separate harm.

Attacks like these constitute a substantial risk to investors as the potential success of attacks could cause meaningful damage to confidence in cryptocurrencies, conceivably resulting in negative price pressures as investors leave the network.

Additional Risks

This discussion simply presents the larger risks to the future utility of the network as we currently see them. It is not meant to be exhaustive and should not be considered as such. As with any investment opportunity it is important to perform proper diligence and know the risks of the market you are investing in, prior to investment.

CITATIONS

1. Wikipedia. *scrypt.* [Online] 18 January 2018. [Cited: 4 February 2018.] https://en.wikipedia.org/wiki/Scrypt.

2. Wikipedia. *Space-time tradeoff.* [Online] 20 December 2017. [Cited: 5 February 2018.] https://en.wikipedia.org/wiki/Space–time_tradeoff.

3. Popper, Nathaniel. *Digital Gold: Bitcoin and the Inside Story of the Misfits and Millionaires Trying to Reinvent Money.* New York : HarperCollins, 2015. 978-0-06-236249-0.

4. Theymos. BitcoinTalk. *BitcoinTalk/Bitcoin Forum/Bitcoin/Development & Technical Discussion.* [Online] 3 October 2010. [Cited: 5 February 2018.] https://bitcointalk.org/index.php?topic=1327.0.

5. Lolcust. BitcoinTalk. *BitcoinTalk/Bitcoin Forum/Alternate cryptocurrencies/Announcements (Altcoins).* [Online] 26 September 2011. [Cited: 5 February 2018.] https://bitcointalk.org/index.php?topic=45667.0.

6. Coblee. BitcoinTalk. *BitcoinTalk/Bitcoin Forum/Alternate cryptocurrencies/Altcoin Discussion.* [Online] 2 October 2011. [Cited: 7 February 2018.] https://bitcointalk.org/index.php?topic=46528.0.

7. GitHub. *GitHub/litecoin-project/litecoin.* [Online] 7 October 2011. [Cited: 6 February 2018.] https://github.com/litecoin-project/litecoin.

8. Coblee. BitcoinTalk. *BitcoinTalk/Bitcoin Forum/Alternate cryptocurrencies/Announcements (Altcoins).* [Online] 9 October 2011. [Cited: 3 February 2018.] https://bitcointalk.org/index.php?topic=47417.0.

9. Litecoin Foundation. *About Us.* [Online] [Cited: 15 February 2018.] https://litecoin-foundation.org/about-us/.

10. YouTube. *SF Bitcoin Devs Seminar: Scaling Bitcoin to Billions of Transactions Per Day.* [Online] 5 March 2015. [Cited: 3 February 2018.] https://youtu.be/8zVzw912wPo.

11. Poon, Joseph and Dryja, Thaddeus. Lightning Network - Scalable, Instant Bitcoin/Blockchain Transactions. [Online] 14 January 2016. [Cited: 12 February 2018.] lightning.network.

12. Antonopolous, Andreas M. *Mastering Bitcoin.* Sebastopol : O'Reilly Media, 2017. 978-1-491-95438-6.

13. Bitcoin Wiki. *Scalability.* [Online] 12 May 2017. [Cited: 12 February 2018.] https://en.bitcoin.it/wiki/Scalability.

14. Bitcoin Core. *Bitcoin Capacity Increases FAQ.* [Online] 23 December 2015. [Cited: 22 February 2018.] https://bitcoincore.org/en/2015/12/23/capacity-increases-faq/.

15. Litecoin Wiki. *Litecoin.* [Online] 18 February 2018. [Cited: 21 February 2018.] https://litecoin.info/index.php/Litecoin.

16. Visa Inc. at a Glance. *Visa.* [Online] [Cited: 26 February 2018.] https://usa.visa.com/dam/VCOM/download/corporate/media/visa-fact-sheet-Jun2015.pdf.

GLOSSARY

Cryptocurrency	A cryptographically secured, decentralized, digital bearer asset
Litecoin	Upper case Litecoin refers to the telecommunications protocol and network
litecoin	Lower case litecoin refers to the native currency running on the Litecoin protocol
Protocol	A set of instructions dictating a common structure of communication between separate parties
Network	A web of interconnected nodes communicating with each other using the same compatible protocol
Nodes	The single unit components of a network
Blockchain	One of the central data structures in Litecoin, containing all blocks ever mined
Blocks	Modular data structures containing valid Litecoin transactions, a reference to the previous block, and a proof-of-work
Proof-of-work	A solution to a computationally expensive task, probabilistically proving that the presenter of the proof has expended computational effort in creating it
Miners	Nodes tasked, through competitive computational work, with compiling Litecoin transactions into blocks and time stamping these onto the blockchain
Mining	Mining refers to the competitive task of expending computational work in order to win the privilege of time stamping blocks onto the blockchain (which is rewarded by the coinbase transaction) and the act of adding a new valid block to the blockchain
Coinbase	The first transaction in a block where the block miner can create new litecoins from nothing and send them to themselves as a reward for mining the block
Backwards Compatibility	A change in software that allows interoperability with the previous version of the software
Soft Fork	A change in software that is backwards compatible
Hard Fork	A change in software that is not backwards compatible

Certification Concerning Research Analysts

The research analyst(s) denoted by an "AC" on the cover of this report certifies (or, where multiple research analysts are primarily responsible for this report, the research analyst denoted by an "AC" on the cover or within the document individually certifies, with respect to each security or issuer that the research analyst covers in this research) that:

(1) all of the views expressed in this report accurately reflect his or her personal views about any and all of the subject securities or issuers; and

(2) no part of any of the research analyst's compensation was, is, or will be directly or indirectly related to the specific recommendations or views expressed by the research analyst(s) in this report.

IMPORTANT DISCLAIMER

Please note that this document is provided on the basis that the recipient accepts the following conditions relating to provision of the same (including on behalf of their respective organisation). Should the following conditions not be acceptable, please destroy this document without retaining any copies.

This document does not contain, or purport to be, financial promotion(s) of any kind. This document does not contain reference to any of the investment products or services offered by members of the CoinShares Group.

Digital assets and related technologies can be extremely complicated. Crypto-currencies can be extremely volatile and subject to rapid fluctuations in price, positively or negatively. Crypto-currencies are loosely regulated and there is no central marketplace for currency exchange. Supply is determined by a computer code, not by a central bank, and prices can be extremely volatile. The digital sector has spawned concepts and nomenclature much of which is novel and can be difficult for even technically savvy individuals to thoroughly comprehend. The sector also evolves rapidly.

With increasing media attention on digital assets and related technologies, many of the concepts associated therewith (and the terms used to encapsulate them) are more likely to be encountered outside of the digital space. Although a term may become relatively well-known and in a relatively short timeframe, there is a danger that misunderstandings and misconceptions can take root relating to precisely what the concept behind the given term is.

The purpose of this document is to provide objective, educational and interesting commentary and analysis in connection with litecoin markets and Litecoin protocol developments. This document is not directed at any particular person or group of persons. This material is solely for informational purposes and shall not constitute an offer to sell or the solicitation to buy securities. Although produced with reasonable care and skill, no representation should be taken as having been given that this document is an exhaustive analysis of all of the considerations which its subject-matter may give rise to. This document fairly represents the opinions and sentiments of CoinShares (UK) Limited ("CSUKL"), which is the issuer of this document, as at the date of its issuance but it should be noted that such opinions and sentiments may be revised from time to time, for example in light of experience and further developments, and this document may not necessarily be updated to reflect the same.

The information presented in this document has been developed internally and / or obtained from sources believed to be reliable; however, the CoinShares Group (which includes CSUKL) does not guarantee the accuracy, adequacy or completeness of such information. Predictions, opinions and other information contained in this document are subject to change continually and without notice of any kind and may no longer be true after the date indicated. Any forward-looking statements speak only as of the date they are made, and the CoinShares Group assumes no duty to, and does not undertake, to update forward-looking statements. Forward-looking statements are subject to numerous assumptions, risks and uncertainties, which change over time.

Nothing within this document constitutes (or should be construed as being) investment, legal, tax or other advice. This document should not be used as the basis for any investment decision(s) which a reader thereof may be considering. Any potential investor in digital assets, even if experienced and affluent, is strongly recommended to seek independent financial advice upon the merits of the same in the context of their own unique circumstances.

CSUKL is an Authorised Representative of Sapia Partners LLP, which is authorised and regulated by the Financial Conduct Authority (FRN: 550103). The address of CSUKL is Octagon Point, 5 Cheapside, St. Paul's, London, EC2V 6AA.

This document is subject to copyright with all rights reserved. Use and reproduction of this document or any parts thereof may be done without permission, however, the following citation should accompany any reference to or other use of the information contained in this document: CoinShares Research Litecoin Asset Highlight - www.coinshares.co.uk


CS