Litecoin Cash: The best of all worlds SHA256 Cryptocurrency

Version 1.0

Sebastian CLARKE [a], Iain CRAIG [a] and Michael WYSZYNSKI [a]
[a] *The Litecoin Cash Foundation, London.* [1]

Abstract. We present a "best of all worlds" cryptocurrency targeting the existing mining community whilst offering practical, everyday features to benefit miners and users alike. Features are cherry-picked from existing currencies and implemented with optimised parameters to provide a cheap, fast and stable, general-use blockchain. The IFO model is used to realise initial monetary distribution, using a popular, mature and well-maintained currency to provide the donor ledger, in order to encourage user uptake and provide for liquidity in the marketplace. Some best practices regarding the IFO model are considered and explored.

Keywords. electronic currencies, cryptocurrency, blockchain, peer-to-peer, IFO

Introduction

Cryptocurrencies require a strong and engaged mining community in order to secure the network and validate the blockchain. In addition, they require a highly engaged user community to drive adoption and public presence.

On a cryptocurrency network, miners are not motivated solely by altruism; they mine to generate revenue and cover the set up and running costs of the mining process. As digital currencies are still a nascent technology, speculation is rife, driving significant market volatility. Miners are therefore liable to shift their mining power to whichever asset will yield the highest returns for their efforts.

A successful currency should be able to respond, therefore, to rapid and significant changes (frequently several orders of magnitude or more [1]) to the total network hashing rate provided by the miners.

In the blockchain community at large (taking into account the many and varied permutations on the central ideas laid down originally by *Satoshi Nakamoto*[2]) mining power is becoming more specialised, via the use of differing Proof-of-Work (PoW) algorithms favouring certain hardware configurations.

Nevertheless, there exists a considerable wealth of mining capability directed to one algorithm in particular: SHA256. This is perhaps not surprising, as it is the PoW algorithm favored by Bitcoin, the "gold standard" in the cryptocurrency world, eclipsing the other "alt-coins" in both unit value and total market capitalisation.

[1] *info@litecoinca.sh*

Using market capitalisation as a measure, there are other demonstrably successful SHA256 based coins, most notably, Bitcoin Cash. However, these currencies are characterised by comparatively slow block times and high transaction fees which are ideal neither for miners nor users of the network.

Against this backdrop another phenomenon has started to occur, of which the aforementioned Bitcoin Cash is the initial progenitor, that of the hard fork, or Initial Fork Offering (IFO).

We believe that the more significant and interesting aspects of this innovation have been overlooked due to the specific circumstances of the first widely known and publicised instance, the fork of Bitcoin Cash from Bitcoin.

This particular fork was marred by political infighting, and arose from philosophical differences over the direction of the development process, eventually culminating in a split of the development team, a hard-fork of the currency and the new currency challenging the parent for legitimacy and supremacy in the marketplace.

We do not believe this process will be typical of many future IFOs and in fact we believe that the more interesting utility of an IFO is its use as a means of initial distribution of financial liquidity in a newly launched cryptocurrency.

The problem of initial distribution in a new digital currency has been traditionally addressed either through the use of ICOs or via "Airdrops", both of which have significant drawbacks, when it comes to both fairness and the extent of distribution.

Keeping in mind that blockchain fragmentation is good for the security and utility of broader cryptocurrency, in the same way that genetic variation is vital for a healthy biological population, we will argue that IFOs are superior to the other methods of initial financial distribution, whilst presenting our coin, Litecoin Cash, as an exemplar implementation uniquely suited to the particular challenges of an Initial Fork Offering.

With a wide and ready pool of mining power to tap, state-of-the-art difficulty adjustment to react to network hash dynamics, a mature and fair distribution, and a modern feature set, tuned to everyday use with fast transactions and low fees we are confident that the legitamacy of our ideas, will be borne out by success in the wider market.

With a view to the future, our team are focused and motivated to use this platform to continue to deliver universal, utilitarian innovations in cryptocurrency to demonstrate and realise its significant potential and use.

1. Initial Currency Distribution in New Cryptocurrencies

In order for a currency to be spendable, there needs to exist some method of distributing it into the hands of potential users. It stands to reason that a currency with a wide and varied distribution, is likely to see more usage than a currency with a narrow or flat distribution, by the simple fact that more people are able to spend it.

How then to achieve this initial distribution of finances in the context of a new cryptocurrency launch? A few strategies have so far manifested.

1.1. Airdrop

Often funded or accompanied by an initial private mining of the cryptocurrency before release to the wider public (a "pre-mine"), airdrops serve to merely deposit the currency

into the wallets of interested parties from some central reserve on a basis that is, though different from coin to coin, inherently arbitrary.

This presents some problems with respect to both the fairness, and extent of the distribution achieved. The supposed fairness of any airdrop distribution obviously varies dependent upon the exact conditions of any particular instance, however, they are certainly susceptible to the whims of human corruption due to the arbitrary nature of the distribution.

They are frequently distributed on a first come, first served basis and this approach naturally favours those closely watching developments in the cryptocurrency sphere, and is also clearly subject to potential nepotism and corruption concerns.

Furthermore, the width of such a distribution is, by its nature, limited only to those who become aware of the offering during the time in which it is active, and, dependent on other conditions and considerations surrounding the launch of such an offering (i.e., publicity, marketing, P.R., budget etc.), could be seen to limit the distribution quite considerably.

Though airdrops can be considered somewhat risk free, as they do not require anyone to part with anything of value to participate, for the above reasons we believe their utility in distribution of financial equity in a new currency offering to be questionable.

1.2. ICO

Initial Coin Offerings or ICOs have garnered some wider press coverage and controversy of late with several well publicised examples seemingly only existing to serve as subterfuge, with disappearing development teams and lost investments commonplace ([3], [4], [5]).

We believe that ICOs are a flawed proposition, suffering from some of the same drawbacks that can plague crowd-funding offerings, but exacerbated and magnified by the vast sums of money involved, and the ethereal nature of the product offering.

The most notable drawback is that a potential participator is required to deposit funds *before* the delivery of the expected value, product or service, and is required to place a great deal of trust and confidence in the team behind the offering. Naturally, this is open to exploitation.

ICOs also suffer from similar problems with fairness and distribution extent that airdrops do. Whilst their distribution is certainly less arbitrary, the width is again limited to those who are able to leverage the necessary funds to participate. How that affects the perceived fairness is a matter of opinion, however, the distribution is also limited in the same way as airdrops, in that one has to be aware of the offering *during the offering period* in order to participate.

We are not arguing that ICOs have no utility, or that there are no legitimate Initial Coin Offerings, but rather, that they must be approached with caution and careful consideration and that the necessary due diligence and research must be performed in order to minimise risk exposure.

Whilst potentially useful then, we consider ICOs to be a sub-optimal method of initial distribution of financial capital for a cryptocurrency launch.

1.3. IFO

Initial Forked Offerings or IFOs ("hard forks") are a more recent trend in new currency offerings. They seek to exploit an existing transaction ledger (i.e., the block chain) in order to provide the initial distribution of a new currency.

In this way, fairness can be proven and guaranteed by the technology, as only the people with correct keys on the old network, can access and redeem the funds on the new network. The developers and controllers of the coin can in no way be accused of being able to unduly affect the distribution of the currency.

With this method, potential participants need not even be aware of the IFO at the time of launch[2] as the funds remain locked to those private keys in perpetuity. It is merely necessary that they have funds on the old network at the time of the *fork block*, the block at which old ledger and new ledger begin to diverge. Claims can be made retrospectively, (in principle at any time after the fork) as long as the control of the private keys is kept.

Depending on the donor ledger chosen, an IFO can provide for a wide and varied initial currency distribution, with potentially many years of previous transaction history serving to apportion the currency amongst the users.

Naturally, this solution is not perfect. In the same way that distribution is limited though awareness in the previous two discussed alternatives, it is limited here through the requirement to hold funds on the donor ledger. However, it is limited to an arguably lesser extent, as many potential donor currencies enjoy wide uptake by the general public.

We find an IFO to offer an unparalleled breadth of initial coin distribution when compared to other approaches, and consider this likely to drive community engagement and adoption.

Consequently, we consider IFOs to have considerable advantages with respect to fairness and distribution extent, over either ICOs or airdrops, and will therefore likely be a natural choice for new cryptocurrency launches in the future.

2. Responding to network hash-rate dynamics

2.1. Mining Mobility

In spite of the increasing diversity of Proof-of-Work algorithms in use in cryptocurrencies, networks are still susceptible to large swings in total network mining power (the *hash-rate* of the network).

These hash-rate dynamics are natural, as miners seek to maximise their returns by validating transactions on the currency which will net them the largest financial incentive. Due to the speculation inherent in a nascent industry such as cryptocurrency, market volatility can be extreme, with this volatility reflected in the variance of network hash-rates.

Cryptocurrencies seek to maintain a generally consistent block time to guarantee performance of the network and this is achieved by the use of a mining difficulty, which dictates how hard or easy on average it is for a miner to perform the necessary computation to validate a block of new transactions on the chain.

[2] being aware of the fork block in advance can confer an advantage, as then it is possible to purchase the donor ledger currency in advance, though this could be mitigated by choosing a fork block in the past.

How, and at what frequency, this difficulty value is adjusted dictates how a given currency will respond to changes in total available hash power.

2.2. Difficulty Retargetting

The frequency with which difficulty is adjusted on a cryptocurrency network is an interesting configuration parameter. Too long between adjustments and the network will be susceptible to short term swings in hash-rate overtly affecting the achieved block time. Too short a time, and (depending on the algorithm used) it is liable to constantly over-adjust to small changes, resulting in an unstable difficulty, and unpredictable, cyclical block times and hence mining rewards.

Adjusting difficulty every 2016 blocks is common, as employed by Bitcoin, Litecoin and Bitcoin Cash[3]. With careful selection of the difficulty adjustment algorithm however, it is is possible to re-target the difficulty every single block, maintaining both mean block time stability and rapid network responsiveness to changes in total hash power. This is the approach as taken within Litecoin Cash.

2.3. Dark Gravity Wave

The algorithm we have chosen to adjust mining difficulty target in Litecoin Cash, is the popular and successful Dark Gravity Wave[6] algorithm first conceptualised by Evan Duffield and implemented in the Dash currency. In brief, it acts as a critically damped harmonic oscillator to respond effectively to logarithmic scale changes in mining power over short periods, as well as roughly stable and constant hash-rates.

Dark Gravity Wave uses multiple exponential moving averages and a simple moving average to smoothly adjust the difficulty. This implementation resolves possible exploits in Kimoto Gravity Well, a related earlier work, by limiting the difficulty retargetting to 3 times the 14 period EMA difficulty average. Our implementation of Dark Gravity Wave allows the difficulty to adjust upwards by 300% or downwards by 60% every block.

This was chosen to allow Litecoin Cash to gracefully cope with the rapidly growing, potentially unstable and certainly unpredictable hash-rate dynamic of a new network undergoing community adoption, as well as to respond effectively to any future shifts in mining power from or to the network.

3. The SHA256 Niche & Mining Power Availability

By following the adage *"What's good for the miners, is good for the network"* we believe that there exists a significant opportunity, for a new SHA256 based coin, tuned for modern, every day usage, and with a built in, mature, mining capacity.

Since SHA256 is used as the PoW in Bitcoin, the most successful and widely adopted of the cryptocurrencies, large volumes of bespoke hardware tuned specifically to the purpose of SHA256 hashing exists. Iterative increases in the power of such hardware, initially via more powerful GPU-based mining farms but now entirely in the hands of ASIC developers, frequently render entire generations of mining systems obsolete by

[3] Bitcoin Cash also incorporates a shorter term, though less influential heuristic, calculated every 13 blocks

the visceral competition for efficiency inherent when mining the worlds most valuable cryptocurrency.

This stock of hardware and hash power represents a significant resource and opportunity on which a new cryptocurrency can draw to ensure the presence of network transaction validation capability.

3.1. Current SHA256 Destinations

The two most popular SHA256 coins to mine are currently Bitcoin and Bitcoin Cash. However, these currencies are not without their problems. Bitcoin, for example, has relatively slow block times, high fees and limited transaction bandwidth. Bitcoin Cash has addressed the transaction bandwidth limitations by introducing larger block sizes, however the block times remain the same at ten minutes, limiting potential transaction confirmation speed.

3.2. Optimising for the Real World

A set of features and configuration parameters have been chosen in order to provide the maximum utility possible for everyday usage scenarios. Litecoin Cash therefore provides a practical set of headline features making it an attractive proposition for miners, users and investors alike.

- **Fast:** Rapid transactions and confirmations with 2.5 minute block times
- **Cheap:** Low friction spending with tiny fees
- **Scalable:** Segwit support and fast blocks provide ample transaction bandwidth
- **Future-proof:** Lightning network support provides instant transactions and epic future scalability

4. IFO Best Practice Considerations

The main concerns when initiating a new *Initial Fork Offering* should be that it remains fair amongst early participants, and that it functions effectively, immediately upon release. With this in mind, a number of steps have been undertaken in order to ensure that Litecoin Cash undergoes as smooth and fair a launch as possible.

4.1. Slow-Start Block Rewards

In order to give all miners an equal chance at early block rewards soon after launch, and to mitigate any undue advantage from simply reacting quickly to the fork, Litecoin Cash specifies a "slow start" control on block rewards. This ensures that block rewards scale up linearly over the first two thousand blocks mined after the fork giving miners plenty of time to bring their equipment online without compromising their potential rewards.

4.2. Effective Difficulty Adjustment

To give consistent mining performance a cryptocurrency must make some effort to respond to changes in network hashing rate[4]. This is particularly true of a new currency

[4]See the 'Responding to network hash-rate dynamics' section for more information

and especially so when there already exists significant potential hashpower available. For this reason, the mining difficulty should be recalculated as frequently as possible, in the case of Litecoin Cash at every block, and a robust retargetting algorithm should be used, in this case, Dark Gravity Wave.

4.3. Simultaneous Full Release

One of the ways that fairness can be ensured during the launch of an IFO is by releasing the software to all participants simultaneously. This ensures that individual parties cannot achieve any advantage by, for example, setting up mining or third party integrations before other people have a chance to access the software, and provides transparency as the creators protect themselves from any accusations of favoritism concerning the software release. This process also serves to prevent any isolated mining of the chain before release by any party, other than the stipulated maintenance fund mined by the creators.

4.4. Replay Attack Protection

In order to prevent the possibility of a valid transaction from either the Litecoin or Litecoin Cash blockchain being a valid transaction on the other chain, transaction signatures are generated in a different way on the Litecoin Cash network.

After the fork block, Litecoin Cash requires that the SIGHASH_ALL signature hash type flag is modified to include a SIGHASH_FORKID value, combined by binary OR.

In addition, Litecoin Cash addresses (generated from the same private key format as Litecoin addresses) feature a different Base58 prefix byte, so that Litecoin Cash addresses will all start with C, in contrast with Litecoin's L. This further helps to prevent user confusion; while the transaction signature changes mean the network will not validate any transaction sent erroneously on the incorrect network, the differing prefix byte and (associated UI validation) will prevent a user even trying to create such a transaction.

4.5. Mitigation of Isolated Mining

A simultaneous full release of all final software to all integrating parties would be the ideal scenario at launch. However, the practicalities of managing such a process necessitates giving preview builds to certain service providers (e.g., exchanges and wallet providers) to ensure the presence of such services at launch time for the smoothest launch possible. However, this can lead to problems whereby potential bad actors might use the preview build, and the publically available pre-fork chain state to try and mine ahead in the hope to push their blocks to the network on launch and claim inflated coinbase rewards.

To mitigate this, a key consensus parameter configuration was kept different between preview and release builds, ensuring that any blocks mined in such a way would be rejected by the network. In particular, Litecoin Cash used the *Slow Start* period, with the value 400 specified in the preview source but 2000 being used in the final release.

4.6. Fair and Transparent Maintenance Fund

Another way to ensure fairness and transparency is to be open about how the maintenance fund is generated and used. Litecoin Cash uses a special block reward defined in the consensus parameters ensuring that the exact maintenance fund amount is rewarded to a vanity address publically visible and hard coded into the source (CashierDaZEsyBQkuvv4c2uPZFx6m2XTgT). This allows any member of the public to watch this address and track the transactions over time, giving visibility into how the maintenance fund is being managed.

5. Relationship to Upstream and Development Roadmap

In order to ensure rock solid features, and timely integration of the latest innovations filtering down from the parent codebases (Bitcoin and Litecoin), it is intended to keep the codebase as close as possible to the Litecoin upstream on an ongoing basis.

Nevertheless, the development team are determined to use Litecoin Cash as a platform for innovation in the cryptocurrency arena, with a focus on every-day utility and security, and will not shy away from breaking away from upstream codebases in order to demonstrate innovation, add value to the network and potentially act as a proving ground for cutting edge functionality and novel concepts, architectures and solutions.

Having a small team can bring enormous benefits in terms of agility: decisions can be made and enacted quickly. The Litecoin Cash team will leverage this strength over the coming months and years to deliver key innovations in cryptocurrency, but in the short term, the focus is on more immediate development necessities. These include:

- Development of official SPV wallet.
- Integration with hardware wallets.
- SPV Server software and Java / JavaScript / Python libraries for integration.
- Atomic Swaps and Lightning network.
- Integration of changes from Bitcoin 0.16.

In the longer term, a number of novel ideas and innovations are being discussed, investigated, and prototyped. However, due to their nascent developmental phase, and the limited development resource available to progress them in the short term, providing any further details at this stage could compromise their successful implementation in what is a very competitive commercial space.

References

[1] *Difficulty control for blockchain-based consensus systems*. Kraft, D., Peer-to-Peer Netw. Appl. (2016) 9: 397. `https://www.domob.eu/research/DifficultyControl.pdf`

[2] *Bitcoin: A peer-to-peer electronic cash system*. Nakamoto, S. (2009). `https://bitcoin.org/bitcoin.pdf`

[3] *Investor Bulletin: Initial Coin Offerings*. US Securities and Exchange Commission (2017). `https://www.investor.gov/additional-resources/news-alerts/alerts-bulletins/investor-bulletin-initial-coin-offerings`

[4] *SEC Halts Alleged Initial Coin Offering Scam*. US Securities and Exchange Commission (2018). `https://www.sec.gov/news/press-release/2018-8`

[5] *Initial Coin Offerings (ICOs): Risks, Regulation, and Accountability*. Chohan, U., University of New South Wales (2017). https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3080098

[6] *Dark Gravity Wave*. Dash Documentation https://docs.dash.org/en/latest/introduction/features.html#dark-gravity-wave