Litheum Litepaper

Clayton Rabenda
clay@litheum.org

Challenge

The Litheum team believes that Full Decentralization can be leveraged to produce a Real Web3.

Our vision for Real Web3 is: 1) the openness, sovereignty, robustness, redundancy, and uncensorability that are the core features of Decentralization and 2) the impact and global scale of the traditional web, i.e. the Internet.

The majority of thought on blockchain scaling has been stuck in the context of the Blockchain Trilemma [TODO citation] which posits that the only way to scale a blockchain is via sharding. This viewpoint is currently steering nearly every scaling solution to sharding, whether it is explicitly called as such or not. But sharding sacrifices the critical qualities of Decentralization (redundancy, robustness, etc) for the sake of scale, a dangerous tradeoff. We see the

proliferation of “Layer 0” solutions and bridges as a resignation to this sad conclusion; 1000 separate chains are 1/1000th as difficult to attack as a single chain. A chain with 100 shards will lose data if only 1% of the nodes are compromised.

In the Litheum team’s view, an ideal solution would be one in which 10,000 miners were able to provide similar performance to modern Networks Applications (backbone IP switches, DNS root servers, reverse-proxy frontends, etc) at either 1/10,000th the speed or 10,000x the cost while remaining 100% Decentralized. This seems like a reasonable expectation but current technology misses this mark by many orders of magnitude.

The Litheum team believes that the Blockchain Trilemma is only applicable to chains which have only incentivized (and thereby decentralized) a subset of their functionality and therefore need to rely on external economic factors (typically volunteerism) to provide those un-incentivized functions of the network.

Specifically, in the Blockchain Trilemma, Decentralization is defined this way:

> *The chain can run without any trust dependencies on a small group of large centralized actors. This is typically interpreted to mean that there should not be any trust (or even honest-majority assumption) of a set of nodes that you cannot join with just a consumer laptop.*

We agree that the chain must run “without any trust dependencies on a small group”; we further agree that this is “typically interpreted” as described. However, this is not a correct corollary. We do not need to be able to join a blockchain with our laptop for it to be trustable and we further point out that even in practice this is rarely done. In practice, although users do not run so-called “full nodes” and do not synchronize the entire chain, they still use those chains, correctly, in a trustless manner.

Scale

Although marginal improvements to scale have been made by projects such as Solana, Avalanche, Cosmos, Near, and others, there is still a large gap between the needs of Real Web3 and what these networks deliver. Additionally, it is questionable whether even this modest amount of scale is safe without fully decentralizing the network.

The entire 10-year-old Ethereum chain can be measured in terabytes. BTC and Cardano are only adding megabytes per hour to their chains. Miners on Solana are told that they should have 1gbps network connections, but there is no mechanism to expand it and no justification for that particular rate or how that rate relates to the overall network’s transaction throughput.

Meanwhile, in the Web2 world, 63,000 searches are processed by Google and Visa handles 65,000 transactions every second, the New York Stock Exchange handles 3M trades and Google AdWords serves 30B impressions and 237M clicks every day. Decentralized technology

has not yet demonstrated a realistic path to something that can have the global impact of the traditional web.

Yet, Bitcoin Miners deploy billions of dollars of infrastructure every year. Bitmain's IPO filings showed revenue of $2.3B between 2016-2018 and public statements have claimed over $5B of revenue in 2021 [TODO add citation to bloomberg article]. Despite this, the chain running on this much infrastructure provides only 100M transactions per year. It takes at least $10 of infrastructure to deliver just 1 transaction per year, the real cost is probably closer to $100.

Ethereum miners spent $15B on GPUs during the 2019-2022 bull market. With Ethereum rarely going above 1.2M transactions per day, this is $34 for 1 transaction per year. If we account for electricity, bandwidth, CPUs, harddrives, and other things, again, it would not be surprising if the total capital deployed was over $100 for 1 transaction per year.

Meanwhile, a $100 NIC can handle 10Gbps. A single core of a commodity CPU can verify 10k secp256k1 signatures per second. $100 of RAM can store a UTXO set for perhaps 40M people. What if it were possible to encourage Block Producers to invest in CPU, memory, disk, and bandwidth instead of only hashing ASICs?

Security

Current consensus designs do not decentralize all the functions (RPCs) which a blockchain needs.

For example, typical incentives do not address the fact that wallets require not only the ability to write to the chain but also to read from the chain. This is a 100% necessary and critical function of a Blockchain. A wallet cannot make a transaction without first reading data from the chain and a user must be able to read data during every use-case. There are many other critical functions like this which are typically not paid for by the blockchain itself.

At Litheum we recognize that a Blockchain is a Network Application, not only a database. A chain of blocks is only a feature of a Blockchain, there are many other functions (RPCs) which must be provided. By providing them all in a decentralized way, Litheum is the only *Fully Decentralized Blockchain*. Full Decentralization means that the network will not rely on any volunteerism or dubiously-motivated 3rd parties to provide any critical functionality.

Full Decentralization and Global Scale go hand-in-hand

The Litheum team has discovered that supporting any scale which meets our definition of Real Web3 on a platform that is not 100% decentralized is simply impossible. This is the origin of the Trilemma.

Not only must the cost of the unincentivized RPCs grow massively to support Real Web3, but the lack of incentivization creates a Free Rider Problem. This drives the chain toward a centralized takeover, and this danger grows as the cost increases (i.e. as the chain scales). Under this game, any miner providing unincentivized functions is at a disadvantage from extra costs. Only a miner collecting 100% of the rewards would rationally pay for those functions. This is why we still see the Web2 Big Data business model within the current Web3 space. A service is provided for free until it has captured a significant portion of the users and has a moat of network effects. This captured group of active users and their data are then turned into revenue. [TODO add citation why decentralization matters]

Centralization: the Danger of Un-incentivized Functions

When Infura went down on November 11, 2020, it took down the entire Ethereum ecosystem. Infura claims to be "serving over 6 billion API requests per day and transferring roughly 1.6 petabytes of data per month". These RPCs (APIs) are *necessary* components of the blockchain that Ethereum's consensus does not pay for. ConsenSys, the parent company of Infura, provides these services for free. Metamask, which is also owned by ConsenSys, relies on Infura, which means that Ethereum's so-called "DApps" rely on the services of a centralized service provider. Of course, Ethereum supporters will point out that a user can configure Metamask to point to their own server, or some other server, which is true, but this shows us why these RPCs stand in the way of scale. Either the user must pay for a 3rd party to run their server or they must run their own. In the former case, you've just replaced the problem with the same exact problem but with a different counterparty; in the latter case the user is now an even bigger burden on the network because they are synchronizing the entire chain rather than simply occasionally querying for the tiny part of it needed for their operations.

> *"If every single DApp in the world is pointed to Infura, and we decided to turn that off, then we could, and the DApps would stop working. That's the concern and that's a valid concern."*
>
> *"[We're] effectively supporting the entire Ethereum DApp ecosystem with the RPC traffic."*
>
> *"Any DApp that uses Metamask also inherently depends on Infura (knowingly, or not). In that sense, nearly all DApps potentially depend on Infura."*
>
> *"We didn't create the problem, we are just a Band-Aid on the problem. We are just providing a solution that is needed."*
>
> – *Infura co-founder Michael Wuehler via CoinDesk*

This effectively invalidates the value-proposition of decentralization.

> *"If we don't stop relying on Infura, the vision of Ethereum failed."*

– Afri Schoedon, release manager for the Parity Ethereum client

It is a problem easy to ignore when a blockchain is small or mining is wildly profitable in comparison to the cost of unincentivized PRCs. As the smart contract leader, Ethereum has run into this problem first, but no Blockchain we're aware of has solved it.

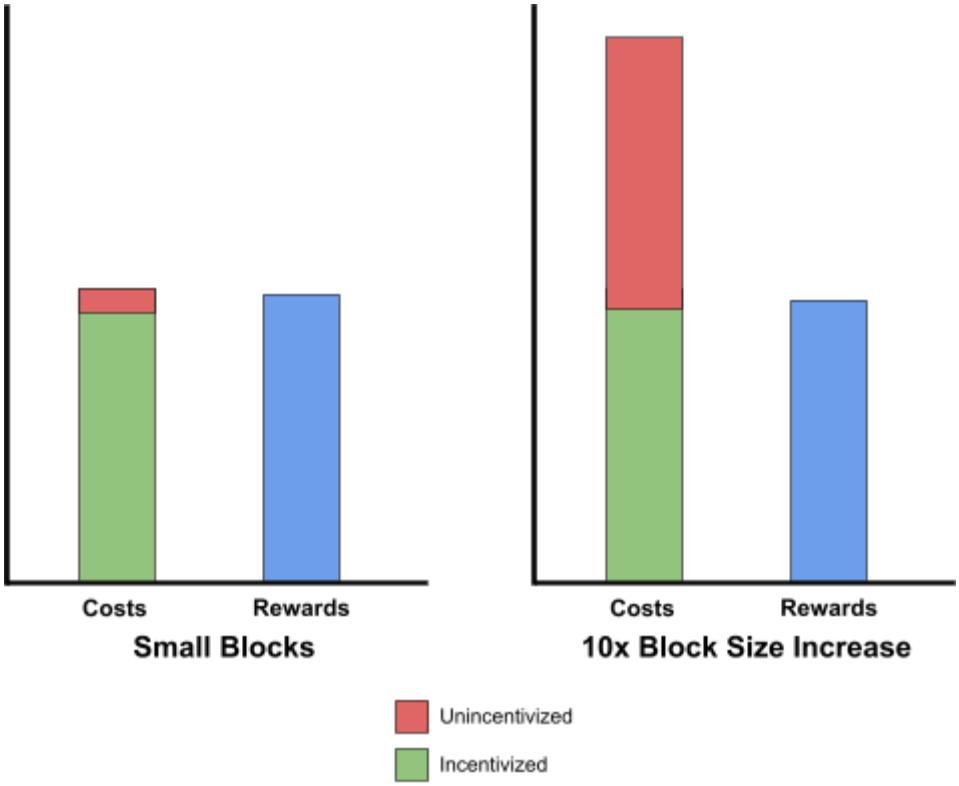
This is also why Bitcoins blocks must remain so small. With small blocks, these problems are marginal enough that they can go unnoticed or can be provided by volunteers. But, if we want a high scale blockchain, that is no longer true. Bitcoin users are encouraged to run a full node. This solution is inefficient, overly costly, and a terrible user experience. All the while the Blockchain is still only capable of delivering very tiny blocks.

Real Web3 is simply impossible in the current paradigm.

The Root of the Problems: Only Hashing is Incentivized

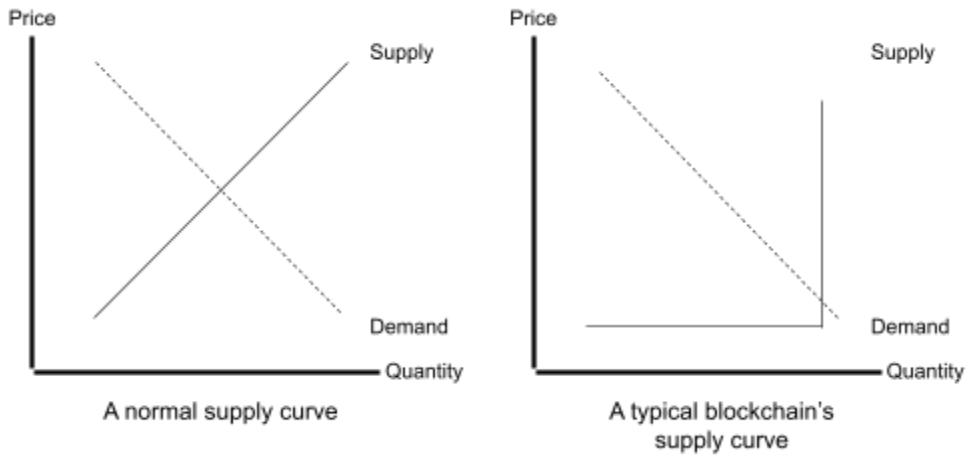
Proof-of-Work only incentivizes a subset of the functionality needed by a Blockchain. Other consensus designs follow this and also only focus on producing the chain, not incentivizing 100% of the blockchain's RPCs. Typically, there is no incentivization for transaction propagation, block propagation, peer discovery, longest chain synchronization (peer synchronization), or even wallet synchronization.

The cost of the incentivized work done on typical chains is independent of the size of the blocks (the cost of finding a difficult hash on an empty block versus a full block is very nearly equivalent). Because of this, increasing the block size is impossible. The unincentivized functionality must be provided by volunteers. If volunteers (i.e. "full nodes") are not willing to provide these RPCs or miners are not willing to accept these costs without compensation, the network will either cease to function or become centralized.



It’s important to note that the cost of finding difficult hashes is only added to the network because it is easy to create a longest-chain win-win nash equilibrium from a difficult-hash-finding algorithm, but that hashing does not actually provide any value to the user directly (other than the perceived value of decentralization itself). The real “work” that transaction-generating wallets want done by the network is the aggregation, validation, verification, and propagation of the transactions.

A Fixed Supply of Block Bytes



The usual solution to the danger of large unincentivized costs is to simply limit those costs. This is why typical Blockchain consensus designs set a maximum block size. This limit guarantees that the cost of unincentivized RPCs does not vastly outgrow the costs which volunteers are willing to bear and allows the network to remain decentralized. Those few chains (for example Monero) which allow this limit to grow are rightfully considered dangerous.

The Litheum Solution: Proof-of-Fees

Full Decentralization via RPC Incentivization
+
Global Scale via Fee-based Difficulty

Full Decentralization via RPC-Incentivization

By redefining what is “difficult” in Litheum’s consensus, “work” becomes that which users actually want done (i.e. the processing of transactions). Litheum Farmers will deploy bandwidth, computation, and memory.

All interactions between parties in a Blockchain require that one party read or write data to another. This is equivalent to considering the blockchain as a network application or that all functionality of a blockchain is done via some RPC.

A wallet must read its Inputs before it can produce a signed Transaction, a Block Producer must synchronize the chain before they can produce a new block, a DEX must know the price of an asset before it can construct a valid swap for a smart contract.

It is perhaps illustrative to consider why, for example, a Bitcoin Miner would want to send a block to a competing Miner. The same problem presents itself even more clearly when considering the propagation of a transaction which is literally as good as money for a Miner who might mine it themself and collect the fee.

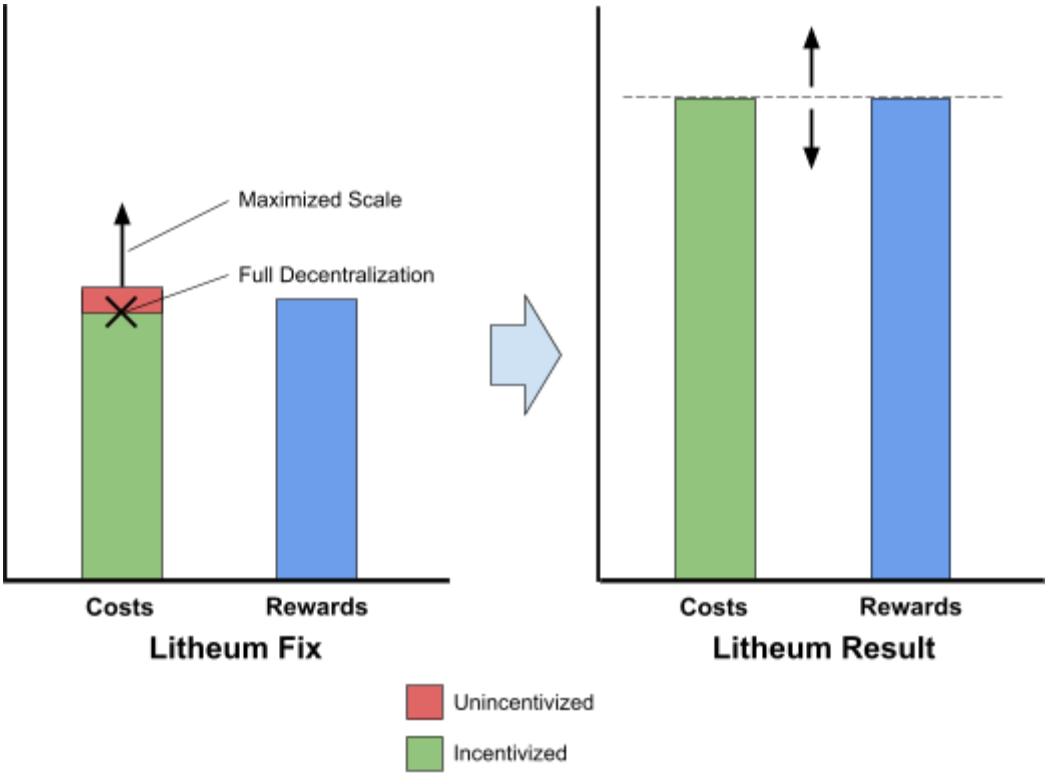
To incentivize all the RPCs needed for a Fully Decentralized blockchain, Litheum has added two mechanisms which are discussed in the Farming section below: Input-Incentivization and Lucky-Hash-Incentivization.

 Global Scale via Fee-based Difficulty

Litheum requires that a valid block must contain some minimum total fees which we call the Block Fee. The consensus targets a block time of 30 seconds (for example), and the minimum Block Fee is decreased or increased if a block is produced faster or slower than the target block time similarly to Bitcoin's Difficulty Adjustment Algorithm.

Doing this in a way which does not incentivize bad behavior is not simple. Typically all data sent in the network is signed and anyone producing bad data or working on multiple forks is penalized. Further details can be found in the Whitepaper.

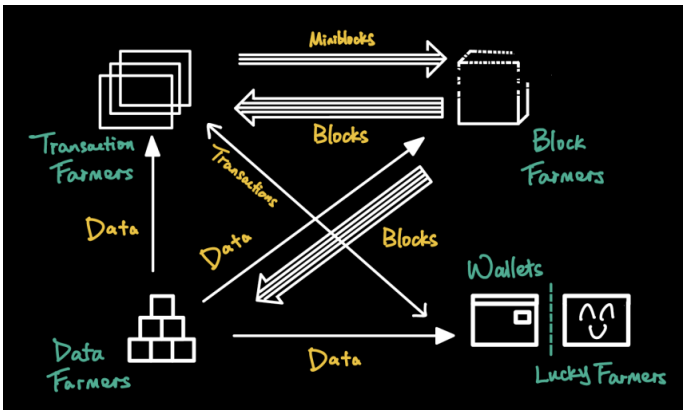
Full Decentralization of all RPCs makes large blocks safe. Using the fee as difficulty allows the production of large blocks to also act as the difficulty in Litheum's consensus. This not only allows the block size to be maximized for scale, it also solves the problem of aligning the work of block production naturally to the real work of processing transactions.



Once unincentivized costs are removed, scale can grow freely bound only by the real cost of the infrastructure which is needed to aggregate, validate, verify, and propagate transactions.

Farming

There are 4 type of nodes which participate in building Litheum's consensus:
Block Farmers, Transaction Farmers, Data Farmers, and Lucky Farmers.

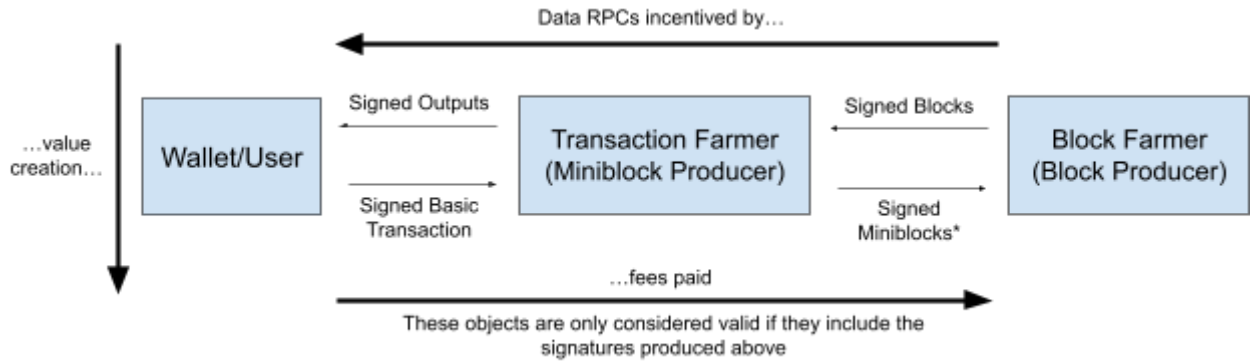


Transaction Farmers collect transactions from wallets and compile them into Miniblocks which are then sent to Block Farmers. This is done for the sake of efficiency and to allow the Block Farmers to work optimally. In conjunction, Transaction Farmers deal with connections from the entire Internet. When a block is made, they split a percentage of the block's fees. There is a maximum threshold of Miniblocks per block. This threshold will be quite small: 10, for example.

Data Farmers on the other hand can share arbitrary data from the Blockchain. How do we incentivize them? This is the purpose of the Lucky Hash Mechanism.

Input-Incentivized RPCs

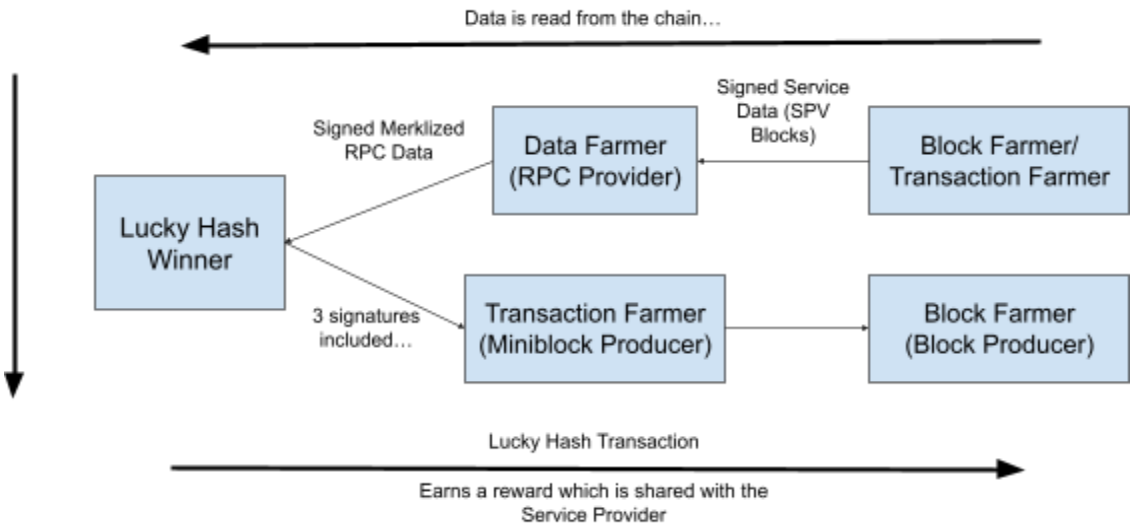
In cases where the data being read from the Blockchain is later used as an Input, the data being read can simply be signed and the provider can later be rewarded. We call these "Input-Incentivized RPCs". This is how Transaction Farmers and Block Farmers are incentivized to propagate blocks and to send data to wallets.



This mechanism incentivizes Transaction propagation, Block propagation, and Wallet synchronization.

Lucky-Hash-Incentivized RPCs

In cases where the data is only read, but never used an input in a transaction, a lottery-like mechanism is used to create incentives. We call this the Lucky-Hash mechanism.



Every wallet holding at least 1.0 LTH is a Lucky Farmer. Lucky Farmers are given chances to find a Lucky Hash each block. For each 1.0 additional LTH held an additional chance is given. If the hash is sufficiently close to 0, similar to PoW's Hash Difficulty, the hash is a Lucky Hash and can be submitted in a special transaction to collect a reward.

Once a Lucky Hash is found, the Lucky Farmer's job is not done. Based on the Lucky Hash, a random Data Farmer and a random RPC are selected. The Lucky Farmer must retrieve a signed copy of this data from the Data Farmer to create a valid Lucky Hash Transaction, which can then be submitted for a Reward.

Every Litheum wallet will have Lucky Farmer features where a user can see any Lucky Hashes which it has recently found. The user has a limited time (perhaps 1 week) to collect the data from the Data Farmer and submit it. Every Litheum wallet should provide this functionality.

The above techniques can be combined to provide a general mechanism for decentralizing any RPCs which are needed. The most critical RPCs can be provided via Input Incentivization, that is the sharing of blocks and

RPC Incentivization Summary

Some RPCs are naturally incentivized without Litheum's mechanisms. For example, in a Proof-of-Work consensus the block producer wants to share a block and other miners want to receive it (note that other miners beside the block producer do not want to share with each other). The table below summarizes the various RPCs critical for a blockchain to function and how they will be incentivized on Litheum. The column named "naturally incentivized" is also reflective of the incentives for those RPCs on other blockchains.

RPCs	*Naturally Incentivized*	*Input Incentivized*	*Lucky-Hash Incentivized*
Transaction Propagation	partial		
Wallet Sync			
Block Propagation	partial	more complete	
Longest Chain Sync	partial	more complete	
Peer Discovery			
Arbitrary Data			

Smart Contracts

The EVM has become the de-facto standard for smart contracts in the Blockchain space. Litheum will integrate the EVM on-chain and perhaps later also as an optimistic rollup on layer two. The appeal of on-chain integration is obvious. However, there is the issue that the EVM requires permanent storage. This will be solved by requiring a minimum balance of LTH per byte of EVM storage. LTH will be locked when EVM storage is used and storage will need to be removed to unlock the associated LTH. The per-byte rate will increase smoothly over time. This not only solves the EVM permanent storage problem but also serves as a commodity-like-base for the value of LTH, which may appeal to some.

Staking

All farming requires stake for punitive purposes. An important distinction from typical Proof-of-Stake systems is that stake is not used as a means of selecting who participates in consensus. Stake only enables the ability to participate as long as the minimum is met. Its use is purely for punitive purposes. Prioritization of block production is based upon the ability of those participants to pass the Block Fee most quickly.

Pruning

Litheum employs a market-driven mechanism to encourage the consolidation and pruning of unspent Outputs. This aligns the reward of block production with the cost across time. Litheum also publishes a merkle hash of any pruned data from the back of the chain into the next new block. This also ensures that all nodes which wish to validate blocks must have a complete copy of the blockchain.

Hardening Difficulty with Inflation

If we consider Bitcoin's source of Difficulty, it's clear that an inflationary reward can be leveraged to increase Difficulty. With a Fee-based Difficulty, it is not straightforward to do this. However, the Lucky Hash mechanism offers a fair entry point for injecting extra fees from oblivion. Simply, every Lucky Hash Transaction comes with an extra fee attached to it. The extra fee can only enter the system by being included into the block's fees and distributed to the other Farmers participating in building consensus. The current plan is to target 2-3% inflation per year.