Lightpaper by

Litheum

Litheum is a new Layer-1 Blockchain with a Novel Consensus Mechanism.

We call it Proof of Fees.

With Proof of Fees, Litheum scales to levels far beyond other blockchains in a safe, fully decentralized way.

We envision everyone on Earth using the Litheum platform multiple times daily. We believe the world needs a true Web3 platform. Web3 means **universal impact** delivered in a **fully decentralized way.**

The Unincentivized Work Problem

In all blockchains, other than just making blocks, some extra work must be done to process transactions. This involves synchronizing wallets and nodes, validating transactions, propagating data, peer discovery, and more.

This work is the valued service which the blockchain provides to all. Users are happy to pay a fee to add their transaction to the chain and holders accept inflationary tokenomics because of the value and service that has been provided.

In a typical consensus design, this work is not paid for. Although wallets pay fees and inflation creates extra funds, those funds don't go fairly to the nodes which provide the work.

Litheum's engineering team calls this problem the "Unincentivized RPCs" (Remote Procedure Calls). It's a problem the industry is well aware of, but it needs to be solved the right way to effect the scalability solution.

The Scaling Problem

Because the unincentivized work is not paid for, it's impossible for other blockchains to scale. As a chain becomes more popular, the cost of providing this work grows. No one wants to volunteer to pay for this work, especially a miner or validator that is competing with others who may cheat and avoid these costs. It's a **prisoner's dilemma that ends at centralization.**

This is the origin of the Scale versus Decentralization problem that has plagued the industry from the beginning. Recently this has become known as The Trilemma.

A $3000 switch can handle 1.5 terabits per second, enough to ship the entire 10 years of Ethereum's data in less than a minute. Each core of the CPU in a typical laptop can verify about 10,000 digital signatures per second. 4TB of RAM is enough to handle wallet data for the entire population of Earth.

What performance will we be able to achieve if we simply remove the danger of unincentivized work?

The Litheum Solution

Litheum's solution is simple.

The unincentivized work is costly to provide. Proof of Fees simply uses this work, rather than hash or stake, as the difficulty of the consensus mechanism. This incentivizes the nodes, which we call Farmers, to provide exactly that which the users want: **processing transactions at scale.** Instead of deploying billions of dollars worth of energy-wasting SHA256 hash, Litheum's Farmers deploy CPUs, RAM, permanent storage, and networking infrastructure that is of value to all in the ecosystem.

By using transaction processing as Difficulty, **Proof-of-Fees incentivizes scale.**

Litheum Security

In the Web3 world, people are seeking the security of Decentralization. Without the danger of unincentived work, a scaled blockchain actually produces the most secure decentralization possible.

It may seem counterintuitive to everyone who is familiar with the current paradigm and the Trilemma, but **large blocks can be more secure** than smaller ones in a fully decentralized context. Proof of Fees theoretically may be the most secure consensus mechanism known to date.

The incentives to produce the consensus must be extracted from the value which the blockchain creates. Users must pay, one way or another, for the nodes to produce the consensus. More usage of the chain will allow more incentives for Farmers.

Litheum total on-chain usage can be perhaps a million times greater than has been seen before. This greater usage will generate more total fees, this increases the difficulty of making a block. A higher difficulty is more secure.

Put simply, more usage leads to more fees which leads to more difficulty (traditionally hash) which leads to more security. Therefore, as long as it doesn't suffer from unincentived work, **a blockchain with bigger blocks should be more secure.**

What Can

Litheum Do?

Litheum is a Scalable GameFi Platform

On-chain interaction for games requires low latency and a low cost per transaction.

Litheum's infrastructure will be able to provide a viable cost for critical services needed by gaming such as real-time data finalization and zero-knowledge fraud detection.

Decentralized Game Designers may also want to put their game's data directly on-chain, Litheum will make on-chain gaming possible. It might be interesting to put a MMORPG's economy entirely on-chain, but the price point must be very low.

Users would love to leverage decentralization for more control over their digital assets. But how much is a user willing to pay to transfer their game skins to another game, sell them, or give them to a friend?

How much would a user be willing to spend to grant their friends access to their gaming world or to decorate their space with NFTs?

Litheum is a Secure Platform for DeFi

- **Low risk of double-spend attacks**
  - Because Proof of Fees is a very secure consensus mechanism, any DEX built on Litheum will mitigate and lower its risk of double-spend attacks.

- **Secured from Sybil-style attacks**
  - Because of the highly scalable and cost effective nature of Proof of Fees, an entire DApp, including the front-end, can be served from the Litheum chain itself. This replaces reliance on centralized infrastructure.

- **Deepest Liquidity**
  - Because DEXes built on Litheum will be able to support a high volume of trading, they will also enable large markets and reduce danger of slippage.

- **Decentralized Order Books**
  - It's important to have equal access to exchange order books, a decentralized order book is very hard to achieve without a highly scalable blockchain.

- **Secure Communication**
  - We also envision a more mature wallet ecosystem that will increase secure peer-to-peer communication by leveraging simple key management.

Litheum's Seamless User Experiences

1. Litheum avoids the need for the use of bridges and multiple tokens solely for the sake of scaling.

2. Litheum avoids complex key management and will reduce the chance of users losing their keys or sending funds to the wrong place.

3. More on-chain capability enables more robust key-management schemes which can help automate and hide some complications like wallet UTXO (unspent transaction output) management.

Innovation Potential with Litheum in the Blockchain Ecosystem

New decentralized experiences which were previously not possible will unleash a wave of creative activity in the Blockchain space.

The team looks forward to the advances that Litheum will afford its ecosystem partners. Litheum empowers the DApps in its ecosystem to deliver decentralization in new, creative ways to their users.

By bringing decentralization to the world, Litheum provides an ideal platform for GameFi DApps, DeFi DApps, and other new Web3 projects to leverage for the next Internet.