Lumo: A Feeless, Instant and Distributed Cryptocurrency, made for the Web

Ryo Akio
ryo@lumo.cash

Abstract. A light, simple, fast, truly scalable and with nearly zero usage cost cryptocurrency, built for and using web technologies. Each user has their own blockchain, allowing them to update it asynchronously and make reliable instant transactions. Despite this, Lumo only needs low space disk usage, to keep network consensus and important features, such as multi-signature, timestamp and arbitrary data, using LumoBox/checkpoint technology.

1. Introduction

The internet and cryptocurrencies have changed how people see and use money. Today, the problem no longer is how to make a decentralized money, or a “digital gold”. The problem now is to reach the everyday people. There are 7 billion people in the world, and most of them still use and trust government money. But… Everyday money cannot take 60 minutes to the merchant be able to trust the transaction. Can’t have fees. Resources are scarce. Every penny matters. A currency must be easily accessible for everyone.

In this paper, we introduce Lumo, a light, simple, fast, truly scalable and nearly zero usage cost cryptocurrency, build for and using web technologies, while maintaining double-spend protection. Lumo’s full node can run on low-power hardware like a Raspberry Pi or your phone, allowing it to be the best currency for everyday usage.

2. Background

As proven by Collin Lemahieu, Bitcoin was not able to be a real currency. High fees, low transaction speed, scalability problems, many characteristics a daily currency **must not** have. So Nano was developed, aiming to solve these problems and break up the status quo, however, unfortunately, it’s still a incomplete solution. Nano does not reach the best of scalability possibilities and loses important features present in many other currencies. Even though it was a genius work, in such a free market environment as it is with the cryptocurrencies, new solutions come to implement, innovate and sculpt ideas.

DAG cryptocurrencies in general, such as Nano, Byteball, and many other projects in development, have done a great job pushing a extremely efficient and scalable technology, but Lumo has come to unify the best ideas of what we have today, and deliver a light as a feather, easy to use, and ideal for web applications. Governments have been extorting and ruining people’s live, through regulations, inflation and heavy taxation. A decentralized currency was one of the first steps to achieve the freedom of every individual, and, since 2009, blockchain scenario has jumped insanely quick through main advances on the currency aspect. Litecoin came to bring a more accessible network, with lighter blocks and solved many problems with Bitcoin on what we call the ‘’PoW mining era’’.

Now Lumo is coming to solve new problems that came with Collin's block-lattice, and make a similar impact that Litecoin made in the past with Bitcoin. It isn't just about making a perfect currency for all situations, it's about empowering individuals to conquer true liberty, true independence. As said by Murray N. Rothbard:

''Only voluntary actions are virtuous actions".

Following this brilliant ethical philosophy, there is no possibility of having a advanced society, guided by moral values, with a centralized organization that spoils people imposing a monopolized currency, manipulated by central banks who work in favor of a oligarchy.

Lumo comes to be a ultimate currency, bringing a strong inspiration in Nano, PascalCoin and Monero ideas, in order to deliver a product capable of changing economics the way it's seen until now. Why do people permit so passively the government watching every step they take in their lives? Individuals can't be property of others, and one of the key things that they need to ensure a safe protection, is what Lumo brings with its features. World will have the opportunity to chase freedom, which it never had before.

3. Accounts

Popular currencies do not think much about accounts, just about addresses, public and private keys, making them just a sum of transaction records received minus transactions sent in a common blockchain. But, accounts are the most important part of a currency. Lumo brings in its technology a new idea.

Each account it's a easy-to-remember number sequence (like 12345-6), with a associated public key, stored in a shared and synchronous LumoBox, like a spreadsheet. Accounts are created on demand, using a reasonable amount of PoW. Representatives (nodes with voting-balance delegated) has the task of including, signing and validating changes to the LumoBox. This idea makes Lumo similar to other currencies, makes it more reliable for exchanges implementation and increases the trust in the network.

4. Transactions

Lumo transactions are simple, to make and to understand. It's just like an e-mail. A record with the amount transacted, the origin, the destination, the timestamp, some optional arbitrary data and signatures. When issued and propagated, they are considered asynchronous and irreversible, just like Nano.

Double spend attempts are not tolerated in any way, are not intentionally created nor propagated by any trusted implementation. When a transaction reach a node, as long as it is valid, becomes irreversible.

When a conflict occurs and attempts to break the consensus of the network, the representatives vote on which of the transactions is valid, just like on Nano. The transaction considered valid for voting by default is the one that came first on the Node.

The default implementations of node and wallet, prioritize sending of transactions to the main representatives, to prevent any form of double spend attack that involves connection poisoning or high-latency attacks.

5. **LumoBox**

As already described in Accounts, LumoBox is like a spreadsheet with a list of all accounts, with number, balance, and public key. From time to time, the representatives will collect all recent transactions, update LumoBox balances and sign everything. Then, the entire transaction history can be immediately deleted, while maintaining network consensus. New nodes that connect to the network pool will rely on known good nodes to make sure they are on the correct network and will blacklist any malicious IPs.

6. **Infinite Scalability**

Lumo can achieve Infinite Scalability since it does not have any type of limitation in the code. Not even Proof of Work is needed for common transactions. Lumo is truly instant. A lot of transactions are not a problem, since nodes and communication with the network will be extremely optimized and transaction history does not have to be stored. The size of the LumoBox will only increase when new users enter the network, not when transactions occur.