LINK MANAGEMENT CHAIN

WHITEPAPER

Revolutionizing Digital Infrastructure

VERSION 1.0.0

contact@linkmanagement.io

June 2018

TABLE OF CONTENTS

1. BACKGROUND

1.1 Internet of Things (IoT)

The Internet of Things (IoT) is an important part of the new generation of information technology and the development of the "informatization" era. IoT is the "object connecting object" internet. It is an extension and expansion of the core, fundamental internet to allow for objects, of any type, to communicate and exchange information among each other. IoT is widely used in the integration of networks through intelligent sensing, recognition technology, pervasive computing, and other communication-aware technologies. It is therefore widely established as the third wave in the development of the world's information industry, following the computer and the internet.

The IoT is an application extension of the internet. It can be thought of as a network, but it is more applicable to think of it as a business and an application. Therefore, application innovation is the core to the development of IoT. Innovation 2.0, with focus on user experience, is the essence of IoT development.

1.1.1 Definition of IoT

The ITU Internet Report, published by the International Telecommunication Union (ITU), defines the IoT as the following: Information sensing through two-dimensional code reading devices, radio frequency identification (RFID) devices, infrared sensors, global positioning systems, and laser scanners. The equipment, in accordance with the agreed-upon protocol, connects any items with the internet, and carries out information exchange and communication. This establishes a network that is intelligently identified, located, tracked, monitored and managed.

According to ITU's definition, the IoT mainly solves the interaction between Thing to Thing (T2T), Human to Thing (H2T), and Human to Human (H2H). However, unlike the traditional internet, H2T refers to the connection between people using common devices and items, and H2H refers to the interconnection between people without the reliance on devices. IoT also solves the problem of the traditional internet's issue with connecting devices. As its name suggests, it is a network of connected items. Many scholars discuss the IoT and often

reference the concept of M2M, which can be interpreted as Man to Man, Man to Machine, or Machine to Machine. Ultimately, most of the interaction between people and machines, and machines and machines are to realize the information exchange between people.

1.1.2 Current Limitations of IoT

In the process of long-term development and evolution of the IoT it encountered the following limitations in the industry: equipment security, personal privacy, structural rigidity, communication compatibility and multi-agent collaboration.

Equipment security is an issue, as exemplified by the Botnets of Things created by Mirai, which was rated as one of the top 10 breakthrough technologies in 2017 by the MIT Technology Review. According to statistics, the Mirai botnets have cumulatively infected more than 2 million cameras and other IoT devices. They were also responsible for several Distributed Denial-of-Service (DDoS) attacks targeting Dyn, an American-based Domain Name Resolution (DNS) service provider, Twitter, PayPal and other popular domains. There are also botnets that enslave IoT devices for mining cryptocurrency, as well as larger and more active http81 botnets.

The concern of personal privacy largely precipitates from the use of a centralized data management structure. This approach of storing data has been exhibited to be insecure and vulnerable to data breaches.

Structural rigidity is questionable since the current IoT is implemented such that data flows are aggregated into a single centralized control system. With the continuous evolution of Low-Power Wide Area (LPWA) technology, it can be foreseen that the future IoT devices will grow exponentially. According to IBM's forecast, by the year 2020, there will be more than 25 billion devices connected to each other. The cost of centralized services to manage this immense number of devices will be unfeasible.

In terms of communication compatibility, the global IoT platform lacks a unified language. This will certainly lead to communication obstructions between multiple IoT devices, and consequently influence multiple competing standards and platforms to be developed. Limitations in multi-agent collaboration exist because the IoT is largely composed of service providers and internal organization networks. In order for collaboration across multiple service providers and peer entities, the cost of establishing trust is high.

1.2 Blockchain

On October 31, 2008, Satoshi Nakamoto proposed a whitepaper on the design of Bitcoin. Since then, blockchain has been operating and captivating interest around the world. Bitcoin, implemented as a primary application of the blockchain, fulfills its original intention as "a decentralized electronic currency system". The production of Bitcoin does not depend on any institution, but it is instead generated by a specific algorithm, and relies on a large number of difficult calculations to ensure the consistency of the Bitcoin network distributed ledger system. Ethereum went a step further and provided us with a generic blockchain framework that can run code with Turing completeness.

Blockchain is the core supporting technology of digital cryptocurrency systems, as represented by Bitcoin and Ethereum. It utilizes data hashing, timestamp records, distributed consensus algorithms, and economic incentives to implement a distributed system where nodes do not require mutual trust. Peer-to-peer transactions, coordination, and collaboration are decentralized to address the high costs, inefficiencies, and data storage insecurities that prevail in centralized organizations. It should be noted that the blockchain technology itself is not a brand-new technological innovation, but a model innovation generated by a combination of technologies (including peer-to-peer communication, cryptography, blockchain data structure, etc.).

1.3 Integrating Blockchain with IoT

The real-life application of blockchain is not limited to mining and bookkeeping. It also plays a critical role in solving the limitations existing in IoT, as well as increasing user privacy and reducing operating costs.

1.3.1 Eliminating Security Issues and Protecting User Privacy

Currently, the IoT is reliant on a centralized service architecture. An example of a centralized system is the smart home. A smart camera and smart sensor are capable of monitoring and collecting user data and aggregating that data to the central server. The central server computes and outputs signals to control all connected smart home appliances, such as opening the door, opening the window, turning on the lights, turning on the air conditioner, etc. The consequence of this centralized approach is that hackers can infiltrate home networks and steal personal data by targeting networked home devices. For example, hackers can use smart refrigerators as an entrance to hijack your home network and personal

computers to steal personal information, account passwords, private photos, and even control other connected devices (ex. smart door locks, smart gas ranges, etc.).

More importantly, even if it is known that the home network is being compromised by hackers, detecting problematic nodes is a challenge for the IoT because there are numerous nodes in the network. The number of data nodes can exceed hundreds of millions, which is virtually impossible to troubleshoot. The overshadowing defect of IoT security is a consequence of the lack of a trust mechanism between devices. All devices need to be verified against the IoT's central database. Once the central system collapses, it will induce substantial repercussion to the entire IoT network, and hackers will be able to gain full authority effortlessly.

The distributed network architecture of blockchain provides a mechanism to maintain consensus among devices without the need for verification with a central database. As a result, if one or more nodes in the distributed network are compromised, the data of the entire network will remain unaltered and secured.

1.3.2 Reducing Operating Costs

In a centralized ledger system, a central server responsible for recording, processing and storing data in IoT. For example, in smart home appliances, such as air purifiers and sensors. These appliances monitor, process, and transmit information in real time. The accumulation of data at the central server can become challenging to process and analyze. More extensive IoT networks have a sizable number of nodes, and ultimately produces an astronomical amount of data. This constitutes steep demands for storage and computing capabilities for the central server. Consequently, traditional servers are often overwhelmed and the operating and maintenance costs are extremely high.

Operating costs are also affected by the low frequency of IoT device replacements. Considering the smart home again, common household smart devices such as door locks, light bulbs, or thermostats are only replaced every few years. This becomes a rather significant problem for device manufacturers. The outdated software and system burden of IoT devices, after long-term, use will bring enormous cost pressures to the management and maintenance of operators and service providers.

Blockchain technology allows smart devices, within the IoT, to transfer data in a peer-to-peer, directly-coupled manner rather than through a central server. This distributed computing approach can effectively dissipate enormous amounts of computational pressure,

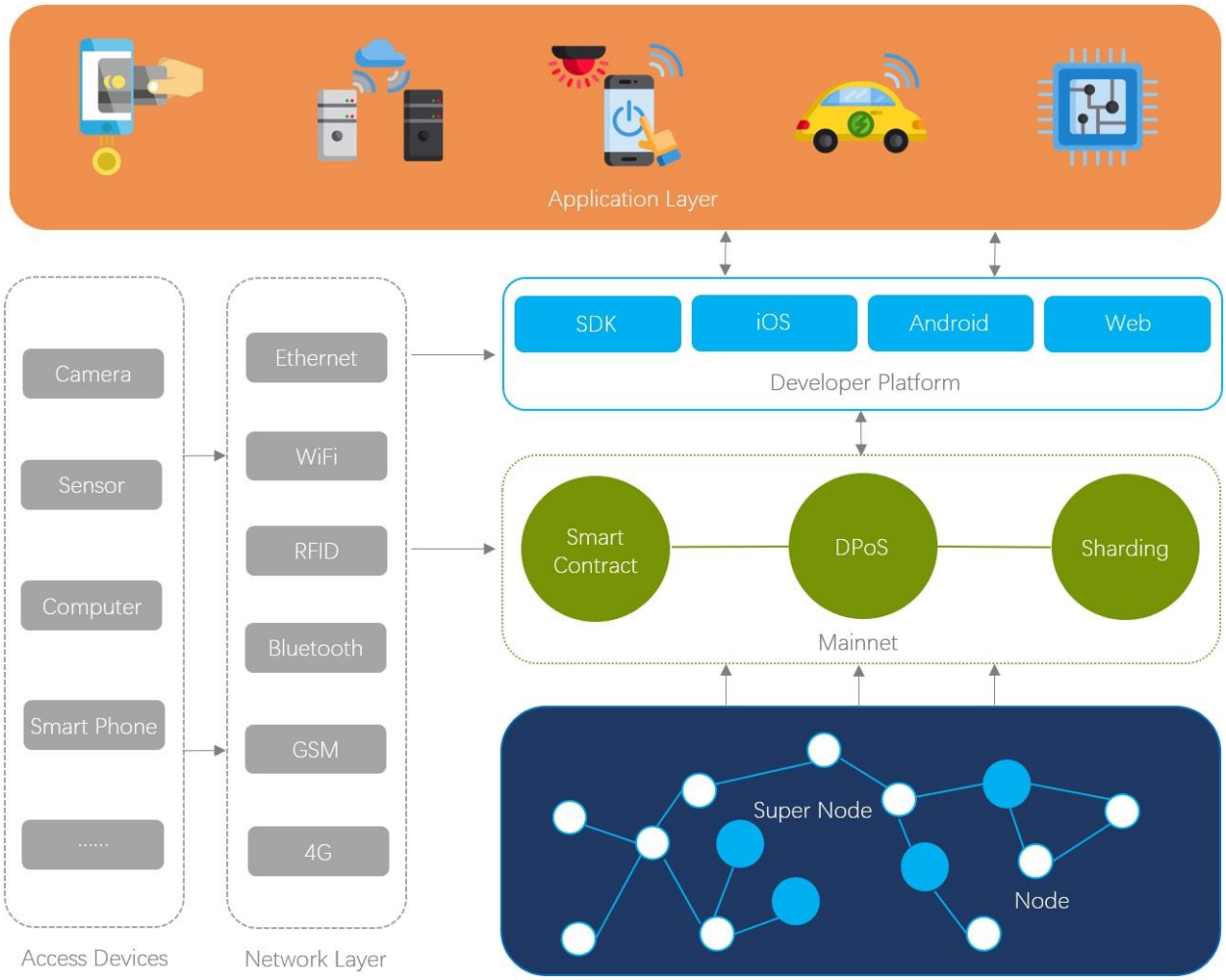
as would be required by a central network approach. Simultaneously, blockchain technology can also take full advantage of the computing power, storage capacity, and bandwidth of idle devices, which significantly reduces the cost of data calculation and storage.

Blockchain's features such as openness and transparency, secure communication, immutability, and multi-consensus will have a significant impact on the IoT. Its decentralized nature will reduce the infeasible operation and maintenance costs of a centralized architecture. Blockchain's characteristics of information encryption and secure communication will reinforce privacy protection. Authentication management and multi-consensus will help identify illegitimate or malicious nodes and prevent them from accessing and acting within a timely manner. The traceability of digital records, distributed architecture, and peer-to-peer features help to eliminate the existing data aggregation clusters on the IoT and promote a horizontal flow of information and collaboration between multiple parties.

2. TECHINICAL OVERVIEW

By leveraging the fundamental characteristics of blockchain, which essentially links transaction blocks as a chain, Link Management (LMM) Chain will be suitable for primitive and sequential data storage. Due to the nature of blockchain, LMM Chain enables data to be verified internally and ensures it is immutable. It also establishes consensus on transactions and status for all involved users in the chain.

2.1. Architecture Overview



Link Management Chain Architecture

2.1.1 Mainnet

The mainnet uses the Delegated Proof of Stake (DPoS) algorithm and has a Turing complete virtual machine, which makes LMM smart contracts more flexible with the actual data. LMM Chain also implements sharding technology to increase network load capacity and provides a solid and reliable foundation for millions, or even tens of millions accessing the IoT.

2.1.2 Developer Platform

The developer platform provides Software Development Kits (SDK) for developers to access blockchains, including multi-version interfaces such as web, iOS, and Android, to provide developers quick and easy access to the mainnet.

2.1.3 Application Layer

LMM chain can be applied to supply chain management, sharing economies, and creating energy exchange economies. The application layer provides users with an interface to interact and manage their specific LMM application.

2.1.4 Network Awareness Layer

Network awareness layer allows IoT devices to access the LMM chain mainnet using a variety of networks types including RFID, Ethernet, WIFI, Bluetooth and etc.

2.1.5 Access Devices

Access Devices, such as webcams, various types of sensors, mobile phones and other types of equipment.

2.2. Delegated Proof of Stake Consensus

Link Management Chain utilizes the Delegated Proof of Stake (DPoS) consensus algorithm to mitigate the potential negative consequences of centralization by using witnesses (usually called representatives). A total of 101 witnesses sign any new blocks before they are registered into the blockchain. These witnesses are voted, for each transaction, by other nodes in the network. By using a decentralized voting process, LMM Chain is more democratic in design than competing systems, while still preserving network correctness and objectiveness. In addition, the voting mechanism eliminates the possibility of untrusted nodes from validating

transactions. The voting mechanism also introduces centralization at the sublevel, which will benefit the transaction efficiency and performance within node clusters under delegated nodes.

This delegated voting approach not only reduces the overhead and transaction costs within the main chain nodes, but also stabilizes the main chain network by removing the encumbered nodes. Hence, the transacting efficiency is significantly improved in the LMM chain compared to the current mainstream Proof of Work (PoW) consensus networks such as Bitcoin and Ethereum. This DPoS approach also enables LMM chain to achieve similar theoretical transaction settlement performance compared to current centralized systems such as Visa and MasterCard.

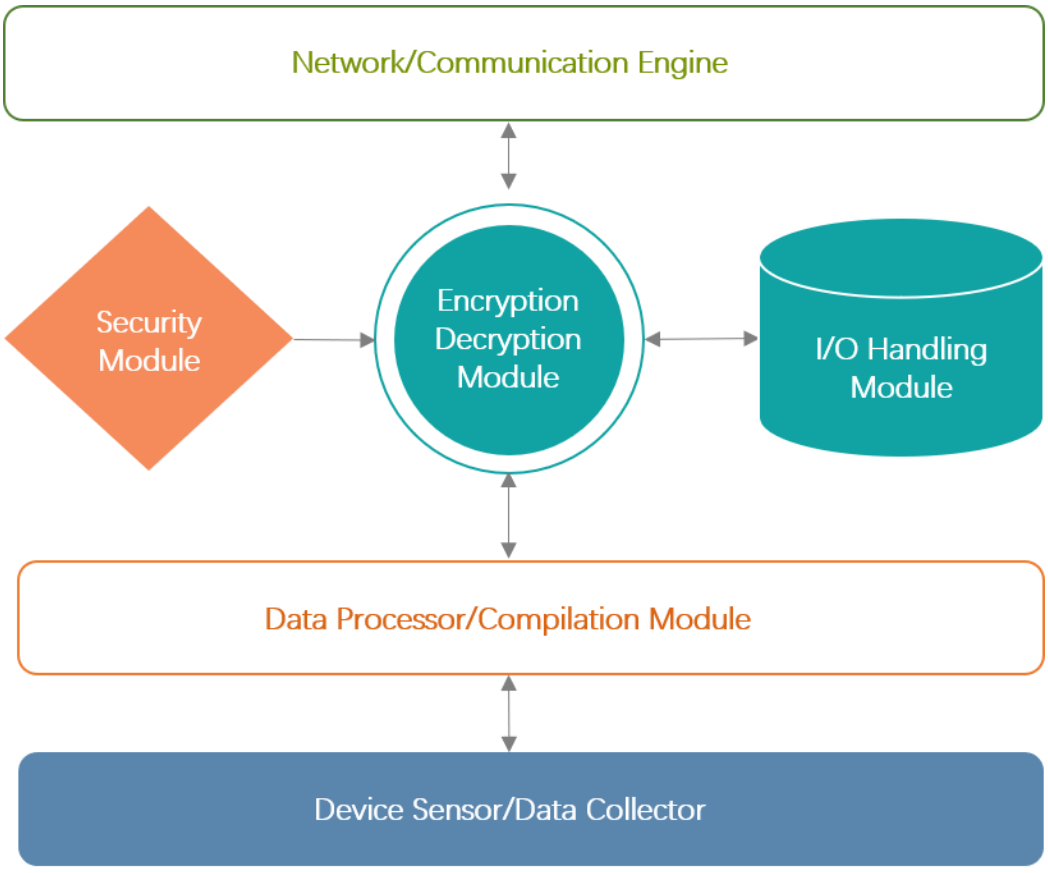
2.3. Rewarding System

In the LMM mainnet, any address with 5 million locked LMM tokens is eligible to validate transactions. Any wallet address with LMM tokens may vote for node candidates. Based on the total LMM token holding amount of all voters for each node candidacy, the top 101 candidates will be elected as the main trusted nodes, and they will be rewarded with LMM tokens.

The rewarding system distributes LMM tokens per block: During the first year of LMM chain's operation, the reward will be 50 LMM/block, reducing to 40 LMM/block at the second year, and so forth. The reward will be reduced each year until it is reaches 10 LMM/block. At this point, the block reward remains constant at 10 LMM/block to ensure the total volume is increased in small increments. (LMM block reward policy may be revised after the main chain is online)

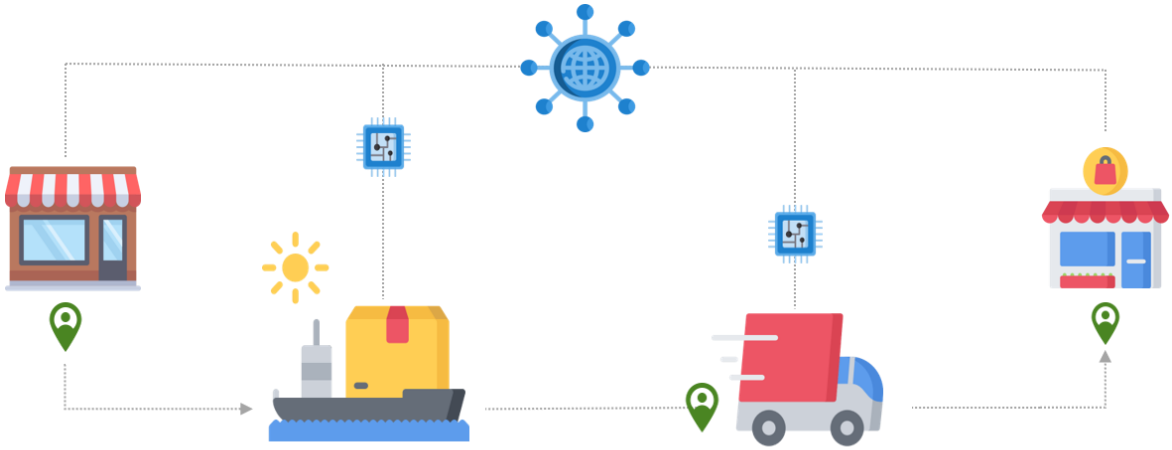
3. APPLICATIONS

Prior to connecting new devices into the system, they will be installed and assigned a public key signed by the device/system user using the LMM application. The security policy, in the application, can be configured such that any preset sensitive information, from the device, will be encrypted with the public key. The key will be stored as transaction metadata and get pushed together with the encrypted device data into LMM's mainnet as a single transaction. In this case, the device/system owner is not required to connect to the device directly or connect to a centralized system to access the device data. Instead, the data can be fetched from the mainnet's nearest or cheapest nodes. The fetched encrypted data can then be extracted from the block and decrypted with the user's private key to retrieve the sensitive information.



LMM Client Application Overview

3.1 Supply Chain Transportation

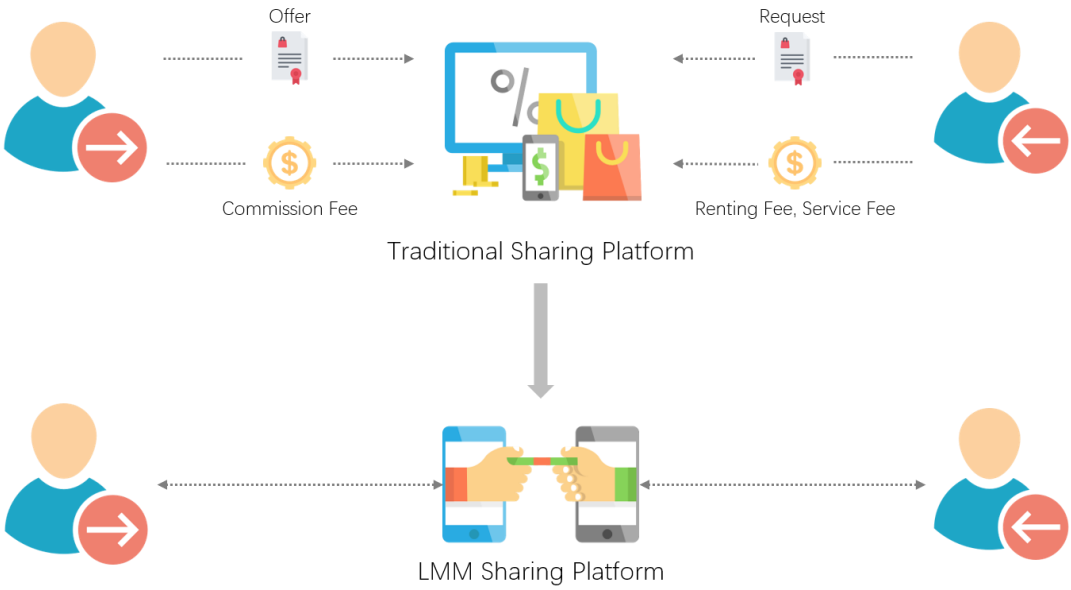


LMM Supply Transportation System

Supply chain management is a fundamental process incorporated in every business. Traditional supply chain transportation is often required to pass through multiple entities. The chain starts at the supplier, then to manufacturers, distributors, retailers, and finally the customer. Many of the information systems between these entities are independent and unrelated to each other. As a result, there is great potential for data forgery, misreporting, or misinterpretation.

If LMM Chain is implemented in this application scenario, sensor devices will be deployed throughout various entities on the supply chain. The data collected, by these devices, are written into the LMM mainnet in real-time (ex. when the ship is docked) and offline (ex. the ship is travelling in the sea). It is tamperproof digital evidence that eliminates data forgery, and also provides transparency of the entire supply chain process. With data collection in real-time, necessary response measures can be promptly made (ex. transporting frozen products; cargo tanks exceeding 0°C require immediate inspection), and the possibility of multi-party cooperation can be enhanced.

3.2 Share Economy 2.0

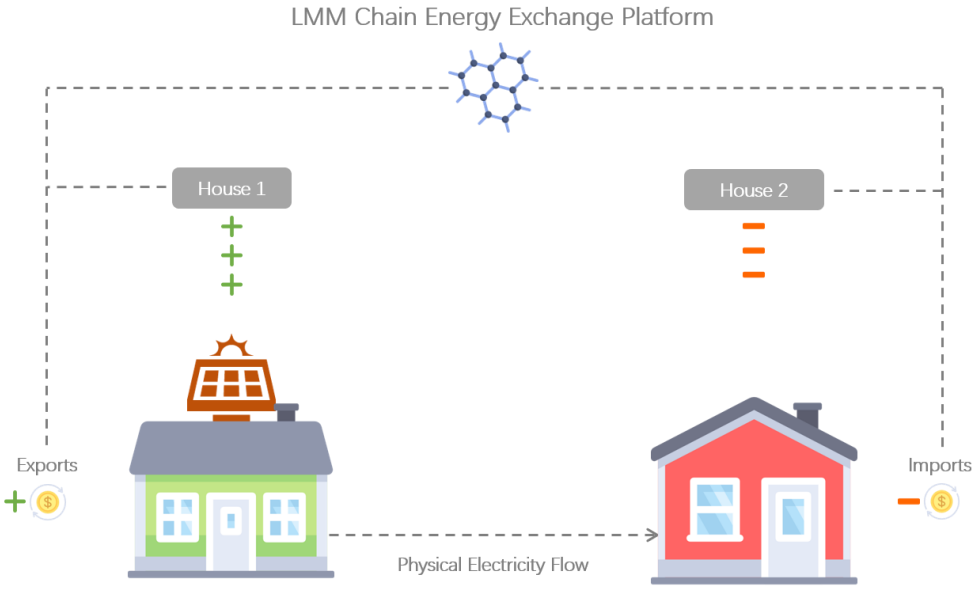


The sharing economy is one of the fastest growing economic platforms recently. The sharing economy allows people to rent their property for others to use. A great example of a sharing platform today is Airbnb, where property owners can rent out their residency to others. This is a commonly preferred alternative for travelers, as it is often a more affordable and/or convenient option than checking into a hotel. However, the traditional sharing economy has its issues. Sharing platforms often require the owner, or both sharing parties, to pay high fees for using the platform. The variety of products available for sharing are also limited to only the sharing platforms available.

One goal of LMM Chain is to establish a universal sharing platform that empowers developers and businesses to establish their own decentralized marketplaces on the blockchain. Our platform will make it more simplified and efficient for organizations to create and manage listings for assets and services. Buyers and sellers can connect through the platform, browse listings, and initiate trading. It also provides a way for freelancers and other independent entities to do business in a decentralized manner. Based on blockchain technology, our implementation allows all users to bypass third-party platform fees through reliable peer-to-peer transactions, and to share any product.

Based on smart contracts, asset owners complete the binding of various locks and assets by setting rent, deposit, and other rules. Through an LMM sharing app, the interested party (end-user) can pay the asset owner the corresponding rent and deposit to obtain temporary ownership. The user is given authority to unlock the locks, specified in the contract, thus obtaining the rights to obtain and use the desired asset. When the asset is returned back to its owner, the deposit is returned. The advantage here is that accurate billing can be processed in real-time according to the billing standards specified in the smart contract.

3.3 Energy Exchange Market



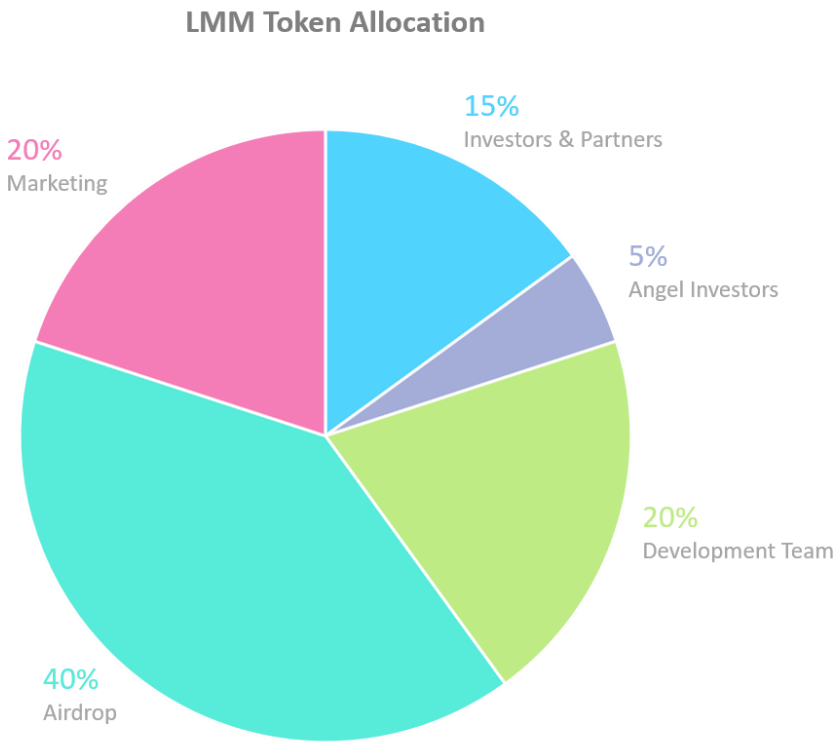
The world energy market is rapidly evolving into utilizing more renewable forms of energy, such as solar or wind-turbine generated energy. Cost of producing renewable energy is also on the decline, empowering consumers to affordably generate their own energy instead of paying additional fees to energy providers. These small-scale energy producers would also be able to trade their energy to other households, essentially creating a microgrid system. However, this type of energy trading market is almost nonexistent; energy exchange contract would have to be drafted and fraudulent claims can be easily forged.

LMM chain intends to make energy exchange practical and economical. By introducing blockchain, peer-to-peer energy trading would become achievable, thus eliminating the need for any third-party energy providers. Consumers would then be able to purchase energy effortlessly by executing purchases through the implementation of smart contracts. Smart contracts will securely create transactions if its predefined conditioned are met. In this case, if I wanted to buy 50 kWh of power at $0.05/kWh, the smart contract would only activate when a seller was willing to meet these conditions. Automatic execution of smart contracts removes the need for authority when delegating energy transfers. Additionally, blockchain can trace logistics from energy producers and consumers to actively adjust energy price based on supply and demand.

4. TOKEN DETAILS

Link Management Chain issues Link Management (LMM) tokens as the means for payment.

Token Name: Link Management Chain Token
Token Symbol: LMM
Token Type: ERC20
Decimals: 8
Contract: 0xe99ddae9181957e91b457e4c79a1b577e55a5742
Total Supply: 2,000,000,000
Airdrop Date: May 27th, 2018 00:00 PST



5. ROADMAP


2017 Q4
Construct Team and Engineer Project
2018 Q2
Commence Airdrop and Release Whitepaper
2018 Q4
Establish Foundational Framework
2019 Q1
Launch Mainnet and Peripheral Components
2019 Q2
Launch VM and Smart Contracts
2019 Q3
Launch IoT, API and SDK
2020 Q2
Partner with Enterprises to Implement LMM Chain

6. DISCLAIMER

This document is only used as the specification of the project and cannot be used as a basis for investor investment decisions. Investors need to make their own choices based on their own objective judgments.

Relevant risks have already been listed. Investors must acknowledge that they are familiarized with the various risks of the project once they invest and are willing to bear the corresponding consequences.

The technical service team does not assume any direct or indirect losses caused by anyone participating in the project.