LIGHTCHAIN
WHITE PAPER

2018 / v1.01

PART 1: ABSTRACT

The emergence of blockchain technology brings us enormous benefits, but the performance and scalability issues makes it difficult for blockchain technology to be widely adopted. We can truly embrace the benefits of blockchain technology only when we solve the performance and scalability issues.

We propose a solution to the performance and scalability problems. Light Chain (LIGHT) is designed to be the world's first double-layer chain. The LIGHT network is composed of one prime-chain and numerous sub-chains. The prime-chain works like bitcoin to provide an immutable and transparent super-ledger while sub-chains provide a fast network under the prime chain, it syncs up with the prime-chain on a regular basis.

PART 2: INTRODUCTION

2.1. Technical

LIGHT's double-layer structure keeps the benefits of immutability and transparency of information, while providing a performance level of 100k QPS (query per second), which is enough for even the high-frequency transactions of 2017. LIGHT's double-layer structure is composed of a prime-chain and numerous sub-chains. The prime-chain is the mother chain, and there is only one prime-chain in LIGHT's network. Sub-chains are independent from each other, and the number of sub-chains can be expanded when necessary. The prime-chain is a decentralized and distributed network that is immutable and transparent to the public. Sub-chains are based on a PoM (Proof of Machine) validation model, combined with an in-memory database, to achieve substantial improvements in performance.

Sub-chain transaction records are regularly synchronized with the prime-chain, at intervals such as 1 hour, 6 hours, or 1 day to ensure the prime-chain has a complete set of transaction records of the entire network. The synchronization process is based on batch

update package. If the package data in the sub-chain has been checked, the prime-chain can update the information without re-checking.

2.2. Economics

Inflation is inevitable in a growing economy. In fact, controlled inflation is symbol of a strong economy. Bitcoin, however, has a deflationary system with a pre-set amount of coins created at the beginning. As bitcoin grows popular, one can benefit more by simply holding bitcoin rather than spending it, and therefore, bitcoin acts more as an instrument for store of value than a medium of exchange, which deviates from its original purpose of a "peer-to-peer electronic cash system."

In LIGHT's double-layer system, the sub-chain is under control of an organization which deploys all machines of the sub-chain; the sub-chain supports its growth through controlled inflation when necessary in its own network. The prime-chain, on the other hand, keeps all transactions immutable and transparent using a decentralized incentive scheme.

As of 2018, most business models still rely on information asymmetry. The emergence of bitcoin, an immutable and transparent decentralized ledger system, is critical to solving the information asymmetry and double-spend problems. However, bitcoin's deflationary nature makes it difficult to support a growing economy and help a society prosper.

The combination of prime-chain and sub-chain design of LIGHT provides us with an efficient, transparent, fair, and economic-friendly model.

PART 3: VISION

And God said, "Let there be light," and there was light. --- Genesis, Bible

LIGHT's double-layer structure enables an immutable, transparent, and decentralized system to scale up and be adopted everywhere in the world for the very first time while remaining economically feasible. We believe LIGHT will be essential for the next social revolution.

PART 4: LOGIC

4.1. Problems

On October 31, 2008, the emergence of bitcoin solved the double-spend problem and introduced the utxo design. In November 2013, Ethereum introduced smart contracts with Turing-completeness. They both made a significant impact towards social improvement, but the inability to scale while remaining economically viable makes it difficult for these crypto-currencies to be widely adopted in the world. The reasons are as follows:

- In each transaction, the record needs to be broadcast to all nodes on the entire network. On the receiving side, miners first store the records locally and then put them into blocks and the blocks are subsequently added to the blockchain;
- Each block has to be validated based on PoW, PoS or other validation methods before it is added onto the blockchain.

As a result, a transaction in a decentralized network may take over 10 minutes to complete in 2017, which limits its application in society to today's fast moving society.

4.2. Analysis

- On the receiving side, an in-memory database is introduced to substantially improve the performance of the temporary storage of received transaction records, which waits for the block validation and then are written onto the block before it is added to the blockchain. On average, the throughput of in-memory database is about 100k QPS (query per second). That is good enough for most of the applications.
- In the validation process, it is necessary to optimize the validation method to obtain the throughput of block generation. The optimized validation would effectively consume the transaction records stored. Otherwise, the overflow would happen in the Database of broadcast requests will be refused directly.

3 existing ways of validation of Blockchain:

Proof-of-Work:

A proof-of-work is a piece of data which is difficult (costly and time-consuming) to produce but easy for others to verify and which satisfies certain requirements. Producing a proof of work can be a random process with low probability so that a lot of trial and error is required on average before a valid proof of work is generated. A PoW system is an economic measure to deter denial of service attacks and other service abuses such as spam on a network by requiring some work from the service requester, usually meaning processing time by a computer. PoW is an outstanding method to secure data, but its disadvantage is also obvious because its computing cost is so expensive.

As mining activity increases, electricity consumption surges. If this trend continues, electricity consumption for the purpose of mining may overtake usage that which is used for regular living purposes, and severely affect human society as a whole. Therefore, the rapid growth PoW must be controlled immediately.

Proof-of-Stake:

In PoS-based cryptocurrency, the creator of the next block is chosen via various combinations of random selection and wealth or age (i.e. the stake). Delegated Proof-of-Stake (DPOS) is robust under every conceivable natural network disruption and even secure in the face of corruption of a large minority of producers. Unlike some competing algorithms, DPOS can continue to function when a majority of producers fail. During this process the community can vote to replace the failed producers until it can resume 100% participation. DPOS is designed to optimize performance of the nominal condition of 100% participation of honest nodes with robust network connections. This gives DPOS the power to confirm transactions with 99.9% certainty in an average of just 1.5 seconds while degrading in a graceful, detectable manner that is trivial to recover from. It is clear that the performance is still under below our expectation.

Proof-of-Machine:

There have been several attempts to build an effective PoM system based on TEE (Trusted Execution Environment), which makes sure that only known devices, with known capabilities and known users are consuming or creating provable data. The TEE provides isolated execution of code on the main processor. When it is powered on, the code that is executed inside the TEE is signed and the signatures are verified before any code executes. Each step verifies the signature of the next step before it runs. As designed, this chain of trust guarantees the "integrity"of the code is verified. The last signature "the health" of the device can be checked assuring nothing has been changed. So the TEE guarantees the security of smart contract and the immutability of the records, which is the kernel requirement of the super-ledger. In fact, the TEE has been supported on both ARM and Intel architecture device for several years.

Since a processor operating in the nanosecond cycle range, it is obvious that the combination between Proof-of-Machine and In-Memory Database would help me obtain the expected performance while the security is guaranteed.

With PoM, a new problem arises. Once implemented, it is as if we have released a powerful deity, making all the decisions in the shadows while overlooking us. However, PoM can be created and so it can be destroyed. Even though, the records on its blockchain is immutable, the chain itself can be destroyed, wiping out any existing records.

4.3. Solution

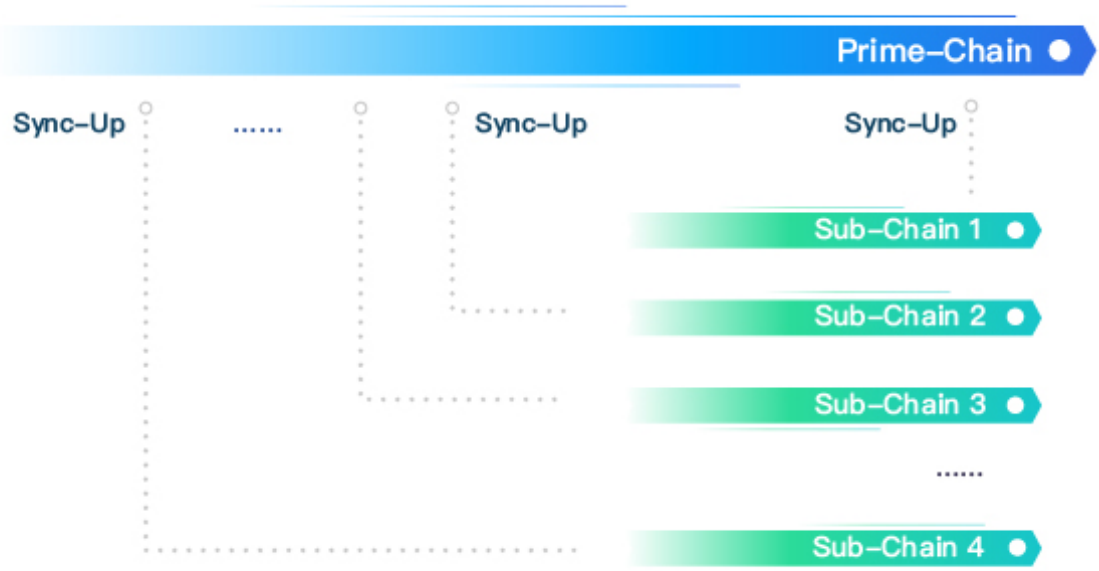
LIGHT's double-layer structure keeps immutability and transparent super-ledger benefits, while providing a performance level of 100k QPS (query per second), which is suitable for all applications including high-frequency transaction.

LIGHT's double-layer structure is composed by a prime-chain and numerous sub-chains. Prime-chain is the mother chain, and there is only one prime-chain in LIGHT's network. Sub-chain is independent from each other, and the number of sub-chain can be extended when necessary. Prime-chain is a decentralized and distributed network that is immutable

transparent to the public. Sub-chain is based on PoM (Proof of Machine) validation model, combined with In-Memory database, to achieve substantial performance improvement. Sub-chain transaction records are periodically synchronized with the prime-chain, such as every 1 hour, 6 hours, or 1 day to ensure the prime-chain has complete transaction records of the entire network. Synchronization process is based on batch update package. If the package data in the sub-chain has been checked, the prime-chain can update itself directly without re-checking.

By solving the scalability and performance problem, LIGHT's double-layer structure can be utilized to all applications in mankind.

Picture insert below:



4.4. Detailed Analysis

4.4.1. Data Integrity

A sub-chain periodically syncs up its transaction records with the prime-chain to ensure a full copy of the transaction records on the prime-chain. When a sub-chain is destroyed, a

synchronization is mandatorily implemented between the prime-chain and sub-chain to record the most up-to-date data.

4.4.2. Data Consistency

Synchronization between prime-chain and sub-chain occurs at regular intervals so that the sub-chain always has the most up to date data.

The steps are as follows:

- Check the status of a sub-chain;
- If the sub-chain exists and is alive, the data is read from the sub-chain;
- If the sub-chain exists but is dead, the date is read from the prime-chain;
- If a sub-chain does not exist, ignore the request.

When a sub-chain is created, its metadata, such as the name, ID, etc, is stored in the prime-chain. When it is destroyed, the info is also recorded in prime-chain.

4.4.3. Isolation of Sub-Chain

In LIGHT's network, sub-chains are isolated from each other. The hardware and software in a sub-chain only exist within the sub-chain and will not be accessible by other sub-chains. Therefore, resources in each sub-chain are isolated from each other, to prevent unnecessary waste in a single-chain structure. This framework design is useful to optimize performance in a system.

4.4.4. Independence of Sub-Chain

In LIGHT's network, sub-chains are independent. Various parties in one transaction must belong to one sub-chain, and no cross-chain transaction is allowed. Therefore, transaction records belong to one sub-chain, and it is unnecessary to store the data in other sub-

chains as it is a waste of resources. If the sub-chain were to be minimized to the extreme, DApp is the smallest unit.

4.4.5. Scalability

In theory, the number of sub-chains can be expanded infinitely, so that LIGHT's network could scale infinitely. Even when the throughput of prime-chain faces limitation, LIGHT's network can continue to expand infinitely by adjusting the update frequency between prime-chain and sub-chains.

4.4.6. Security

Synchronization process is based on smart contract batch update package. If the package data in the sub-chain has been checked, the prime-chain can update itself directly without re-checking. Therefore, LIGHT's security mainly depends on its sub-chains.

4.4.7. Distribution and Concentration

LIGHT's prime-chain is an immutable, decentralized, distributed super-ledger. Sub-chains maintain a high-level of performance as its TEE is deployed by an organization.

The combination of the distribution and the concentration effectively builds a high performance super-ledger that is immutable and transparent to the public.

4.4.8. Traffic model

In the blockchain, the traffic model of the super-ledger follows the traditional one with multiples reading on one writing. The writing is broadcast to all nodes in the network. That is wasteful method for achieving security and backups. In general, the data backup is implemented in the intranet rather than an extranet. It is effective for reducing the cost of broadcasting when the entire network is split into several subnets. In a single layer network with MxN nodes, we need to send broadcast messages to all (MxN-1) nodes for the backup. When the network is split into M subnets, each of which contains N nodes, we only need to

broadcast the record to all nodes within a subnet and the backbone nodes in the parent network. Finally, the total node number for backup is reduced to (N-1) + (M-1). Obviously, since LIGHT network is split into one prime-chain and numerous sub-chains by design, it could effectively reduce the writing cost of broadcast.

4.4.9. Incentive Mechanism

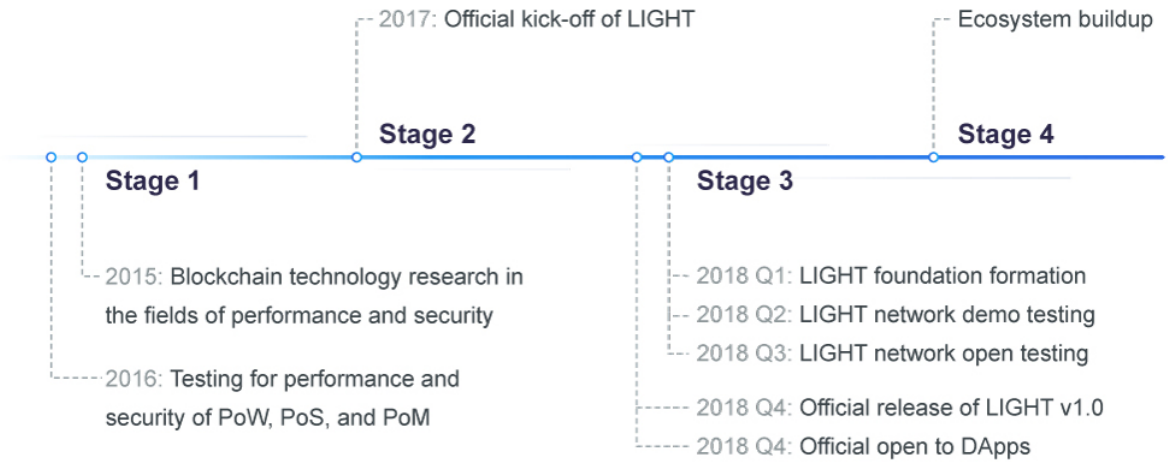
In a traditional design, incentive is the foundation for a decentralized and distributed network. In LIGHT's double-layer structure, its prime-chain keeps such incentive scheme, so that the participants are motivated to build their nodes. The sub-chain is under control of an organization which deploys all machines of the sub-chain, and therefore no incentive is necessary in the sub-chain.

PART 5: ECONOMIC MODEL

In LIGHT's ecosystem, we preset a constant number of Light Coins.

- Similar to the bitcoin and Ethereum systems, miners are rewarded by Light Coin through PoW on the prime-chain;
- Gas is burned every time the sub-chain syncs up with the main-chain. The gas is rewarded to miners;
- A certain number of Light Coins must be pledged when a sub-chain is created. The pledged Light Coins can be used as Gas in the sub-chain, and the number of LIGHT Coins pledged grows over time.

PART 6: ROADMAP



STAGE 1

2015: Blockchain technology research in the fields of performance and security

2016: Testing for performance and security of PoW, PoS, and PoM

STAGE 2

2017: Official kick-off of LIGHT

STAGE 3

2018 Q1: LIGHT foundation formation

2018 Q2: LIGHT network demo testing

2018 Q3: LIGHT network open testing

2018 Q4: Official release of LIGHT v1.0

2018 Q4: Official open to DApps

STAGE 4

Ecosystem buildup

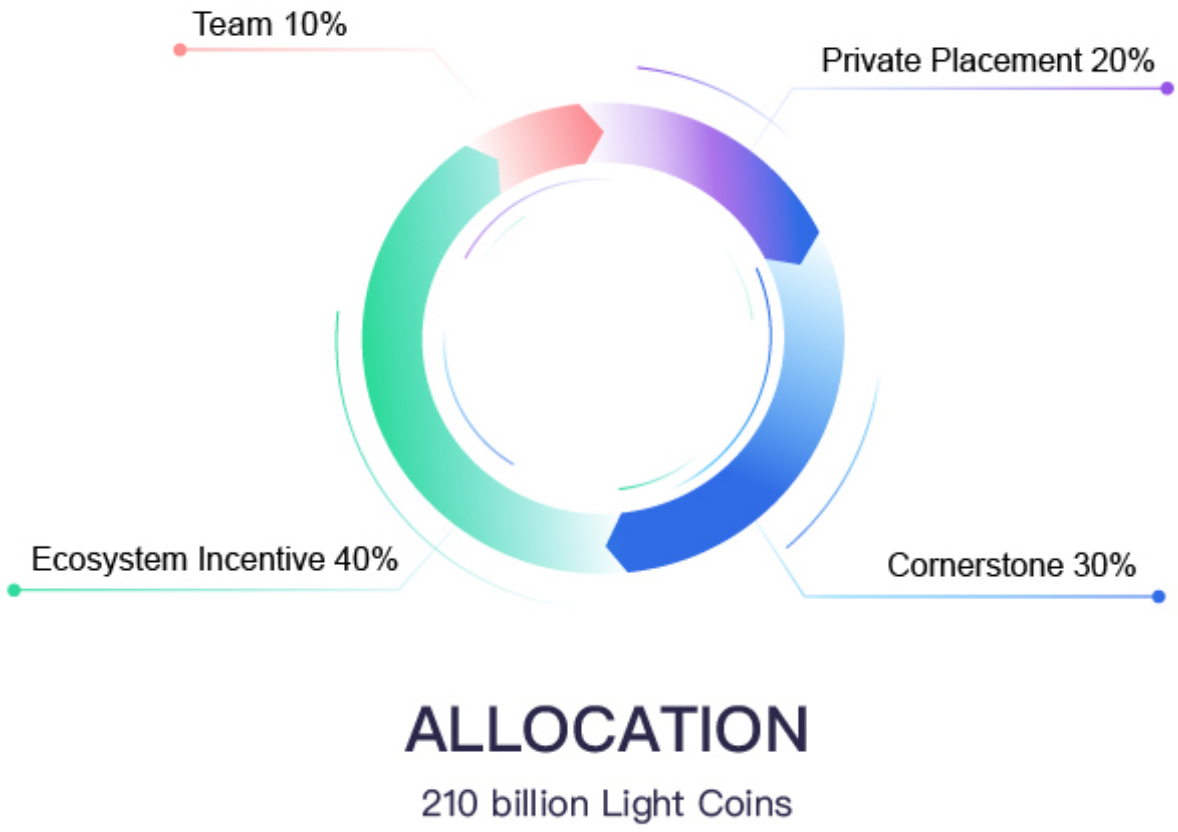
PART 7: LIGHT EXCHANGE PLAN

1. Detailed:

Total amount of LIGHT is 210 billion and is allocated as below:

- Cornerstone Placement: 30%
- Private Placement: 20%
- LIGHT ecosystem: 40%
- Team: 10%

Picture inserted below:



2. Time:

January, 2018

3. Coin Swap:

Light Coin can only be swapped with ETH.

PART 8: TEAM INTRODUCTION

LIGHT CHAIN

The RD team of LIGHT is comprised of more than 40 computer scientists and engineers who are very experienced in blockchain technology, cryptography and digital currencies. The core team has led the development of several world-famous big data storage and processing systems, each of which contains more than 100 thousand servers. Currently, there are 21 developers led by Jason JIA in the core team of LIGHT, whose resumes are follows.

PART 9: LAWS AND REGULATIONS

9.1 Operation Entity

The LIGHT Foundation is a non-profit entity established in Singapore. Our mission is to keep LIGHT ecosystem open, fair, transparent to the public. The LIGHT Foundation is approved by the Singapore Accounting and Business Management District (ACRA) and is governed by the Singapore Companies Act, which is run independently of and independent of the Trusteeship Board or Management Committee and is owned by a suitably qualified trustee of the Foundation Outside the government.

9.2 Disclaimer

LIGHT Foundation is a non-profit organization. Light Coin owners has the right to use in it in the LIGHT network. LIGHT does not promise or guarantee anything beyond the scope of this whitepaper.

PART 10: RISK

10.1 Policy

At present, the regulatory policies for the blockchain projects and the financing of swaps are still unclear. There is a certain possibility of participants losing their investments due to policy reasons. For the market risk, if the overall value of the digital asset market is overestimated, then the investment risks will increase and participants may expect the growth of swap projects to be excessive, but these high expectations may not be realized.

10.2 Regulation

Digital asset transactions including Light Coin, are highly risky. As there are not any clear regulations in the field of digital asset transactions, there is a risk that the price cryptocurrencies may boom or bust due to to market manipulation. After individual participants enter the market, In the absence of experience, it may be difficult to withstand

the asset shock and psychological stress caused by market volatility. Although academics, governments and media have caution the general public about the risks of involved in investing in cryptocurrencies from time to time, there are still no clear formal regulations. Therefore, such risks are difficult to be effectively controlled.

10.3 Team

Currently, there are numerous blockchain technology teams and projects, there is a strong market competition and project operating pressure from fierce competition. Whether the Light Coin project can break out as one of the few outstanding projects and is widely recognized is not only linked to its own team capabilities and vision planning, but also influenced by its competitors in the market. Light Coin founders bring together a host of talents with both vitality and strength, attracting experienced engineers in the area of blockchain. The stability and cohesion within the team are crucial to the overall development of the Light Coin. In the future development, some core personnel may leave from the team and the internal conflict within the team, which may cause the LIGHT project adversely affected.

10.4 Technical

First of all, the project is based on cryptographic algorithm, and the rapid development of computer technology is bound to bring potential risk of blockchain cryptography being cracked. Secondly, technologies such as blockchain, other forms of distributed ledger, decentralization and disagreement support core business development, The LIGHT team cannot fully guarantee the technical deliver; Thirdly, during the process of project update and adjustment, there may be some loopholes that can be remedied by issuing patches, but the degree of impact caused by the loopholes cannot be foreseen.

10.5 Security

A high-standard of security is essential for LIGHT. As the token is anonymous and difficult to be traced, it may be used by criminals or hackers for criminal activities. Other potential risks may exist while blockchain technology continues to grow rapidly. LIGHT coin owners should read and fully understand LIGHT's solution, theory, technical framework, team background, etc. Light coin owners should participate in the coin swap with reasonable expectations.

10.6 Disclaimer

This white paper is for internal use only. This document is for the informational purposes only and the contents of this document are for information purposes only and do not constitute any investment advice, solicitation or solicitation of the sale of stocks or securities in LIGHT and its related companies.

Such invitations must be made in the form of a confidential memorandum, subject to the relevant securities laws and other laws. The contents of this document may not be construed as compelled to participate in the exchange. Nothing in this White Paper may be considered as participation in the exchange, including the requirement to obtain a copy of this White Paper or to share this White Paper with others. Participating in the exchange means that the participants have reached the age criteria and possess complete civil capacities. The contract with LIGHT is true and valid. All participants signed the contract voluntarily and had a clear and necessary understanding of the LIGHT before signing a contract.