Luther

lth.one

A MODULARIZED BLOCKCHAIN INFRASTRUCTURE

White paperV1.0

Catalogue

In the field of blockchain hardware, the Chinese companies show absolute advantages. Most of the global blockchain hardware is produced by Chinese manufacturers. Besides, the world's top three blockchain hardware equipment vendors - Bitland, Jianan Zhizhi and Yibang Technology are Chinese companies. Under the arms race of computing power, by relying in stronger blockchain hardware computing power, the companies may grab more market share. The chip's design and R&D capabilities are decisive factors in this arms race. Therefore, it has greatly promoted the innovative development of China's special chip design industry.

In China, there are more than 450 blockchain companies with blockchain business as the main business, and the number is still growing in an explosive way.

Blockchain technology is not only favored by startups but also by Internet giants. Internet giants have expanded their blockchain business and quickly promoted the growth of China's blockchain industry. At present, Internet giants such as Tencent, Alibaba, Baidu, and JD have joined the research and scene application of blockchain technology.

Tencent builds leading enterprise-level blockchain basic service platform based on Trust SQL core technology. Currently, Tencent blockchain has landed on the supply chain to finance, medical care, digital assets, logistics information, forensic certificates, public interest tracking and other scenes. For instance, Tencent, based on real transaction data in the supply chain scenarios, builds the "Tencent blockchain + supply chain finance solution" through Tencent's blockchain technology and operational resources, which fundamentally improves the financing dilemma of small and micro enterprises, and assists in the transformation and upgrading of local industries.

Alibaba's blockchain-based decentralized, distributed storage, and tamper-resistance features have landed on several application scenarios, including public benefit, authentic traceability, traceability of rental properties, and mutual insurance. Besides, the number of patent applications has reached nearly 80.

Baidu Finance, together with Huaneng Trust and Chang'an Xinsheng, has landed the first order of blockchain technology support securitization project and blockchain technology support exchange ABS project.

JD builds "JD blockchain anti-counterfeiting retrospective platform" by using the blockchain technology, and accurately traces the existence proof quality from solving the pain points of the product, so that all production, logistics, sales and after-sales information is shared, the complete and smooth flow of information is jointly built. In

addition, the blockchain technology is used to solve the trust problem of ABS participants, to complete the transaction on the blockchain system's architecture, and confirm the ownership and authenticity of assets.

The influx of giants has injected new momentum into the development of China's blockchain industry. The industry is poised to take off and will rise rapidly by the new wind of the era.

Although the blockchain is still in its infancy, it has already attracted a lot of talents to the wave of blockchain startups. Many famous traditional VCs have already begun to lay out the blockchain, and the blockchain is the hot spot to now. We should devote ourselves to the tide rather than watching the tide by the shore.

II. What Is Luther?

Luther is a modularized and high-efficiency blockchain infrastructure. LutherChain is not only a public blockchain infrastructure, but also a consortium blockchain infrastructure. Therefore, LutherChain applies to entrepreneurs that establish public blockchain, as well as enterprises, groups, banks and even governmental agencies to establish consortium blockchains.

(1) Public Blockchain

Public blockchain is known as BTC, ETHEREUM or other chains. Public blockchain is open to everyone, so anyone can participate in or join the node. All data is open by default;

At present, China's technology is at the world's advanced level in the field of the public blockchain, and many international public blockchains have been born, such as the famous NEO and QTUM.

(2) Consortium Blockchain

Consortium blockchain refers to the blockchain in which several institutions participate in the ledger keeping, that is, consensus among the members of the alliance is achieved through mutual trust between multiple centers. The data of the consortium blockchain only allows the member nodes in the system to read, write and send transactions, and record the transaction data together.

As a basic component supporting distributed business, the consortium blockchains can better meet the requirements of multi-party cooperation and orderly development in

distributed business. For example, the consortium blockchains is more suitable for transactions and settlements between organizations. Similar to inter-bank transfers and payments, it can create a good internal ecosystem to greatly improve efficiency through the use of consortium blockchains.

Compared with the public blockchain, the consortium blockchains presents advantages in high availability, good performance, programmability and privacy protection. It is deemed as "partially decentralized" or "polycentric" blockchain. The consortium blockchains streamlines the number of nodes and enables the system to operate more efficiently and at a lower cost. In addition, the number of transactions that can be confirmed in a unit of time is much larger than the public blockchain, so it is easier to land in real-life scenarios. What's more, relative to the public blockchain, the very important feature of the consortium blockchains is the node access control and national security standards support, which ensures that the certification entry and the formulation of regulatory rules meet the regulatory requirements and the transaction is accelerated on the basis of trust and security.

III. Why Was Luther Born?

The present blockchain technology has the "impossible triangle", namely, it cannot meet the three requirements of "efficiency, decentralization, and security" simultaneously. Specifically:

(I) The pursuit of "decentralization" and "security" cannot achieve "high efficiency and low energy". The Bitcoin blockchain technology is an extreme pursuit of technological combination that seeks decentralization and security.

From the perspective of data structure, it adopts "block + chain" structure with a timestamp. It has security advantages in traceability and tamper resistance, and it is easy to synchronize data in a distributed system. However, if it is necessary to query and verify the information, traceability and tamper resistance should be involved, yet traversal is an inefficient query method. In data storage, each node downloads and stores all data packets, and uses strong redundancy to obtain strong fault tolerance and strong error correction abilities, not only making the network democratic and autonomous, but also bringing huge verification costs and storage space loss. It does not increase the overall storage capacity via the distributed storage as a distributed database does, but simply adds replicas. As the content carried by the blockchain technology increases in the future, the storage space of a single node will be problematic.

In concurrent processing, the Bitcoin blockchain technology only allows one "miner" eventually to obtain the right of ledger keeping and establish a transaction

block. This mechanism can ensure the safe and robust operation of a democratic network in an effective manner, but it is essentially a serial "write" operation of the entire "chain" that owns all data. For the relational database, the data is divided into several sheets, records in several sheets or sheets can be locked only based on the data involved in the operation, whereas other sheets can still be processed concurrently. By contrast, the serial operating efficiency of Bitcoin blockchain technology is much lower than that of ordinary databases.

In the content verification, Bitcoin blockchain allows each node to own all contents and hashes all contents in the block simultaneously, enhancing democracy and security. However, this holistic hash design idea means that data cannot be stored as an address reference. Otherwise, the information stored on the referenced address may be tampered because it is not hash-checked. As a result, Bitcoin blockchain technology lacks efficient expandability, and there are efficiency issues in processing large-scale content.

(II). "Decentralization" cannot be fully implemented if "high efficiency and low energy" and "security" are pursued

From the perspective of "consensus mechanism", in order to solve the low work inefficiency of workload proof method adopted by Bitcoin blockchain under the premise of ensuring the "security", Proof of Stake (POS), Delegated Proof of Stake (DPOS) and other mechanisms are adopted. However, whether it is POS based on the network rights representative or DPOS achieved by voting with 101 delegates, they are actually a concession to "decentralization", and partial centralization is formed. A typical example is 21 super nodes of EOS, which is to partially sacrifice "decentralization" for the "high efficiency and low energy".

Similarly, in the evolution of the blockchain technology, in addition to the public blockchain technology represented by Bitcoin, the consortium blockchains technology and private blockchain technology are also derived.

The consortium blockchains technology allows ledge keeping only at preset nodes, and the added nodes should be subject to application and identity authentication. Essentially, this blockchain technology is a compromise of "partial decentralization" or "multi-centralization" while ensuring security and efficiency. However, the establishment of block with the private-chain technology is in the hands of an entity, and the read permission of blocks can be selectively opened. For the sake of security and efficiency, it has completely evolved into a "centralized" technology.

(III). Pursuit of "high efficiency and low energy" and "decentralization" must be at the cost of "security"

An extreme case is video player based on P2P (Peer-to-Peer). In the past, when the number of online audiences increased, the video server based on the design of the central server would be slow due to the heavier load. In order to improve efficiency, P2P video player is designed so that a node can continuously download data to others in the meantime of downloading and watching video files. Each node is not only a downloader but also a server. The sharing of resources is no longer dependent on the "centralization" model of the central server.

At the same time, since the video has 24 frames per second, the partial corruption of a small number of images does not affect too many visual senses. However, image delays due to data verification are unacceptable. As a result, P2P video player sacrifices "security" and allows a small amount of error in the transmitted data. In such a decentralized network, the more nodes are involved, the faster the data is transmitted and the more efficient the dissemination is. Of course, data errors are unacceptable for the rigorous financial industry. Besides, security is also a top priority for the financial industry.

In a word, according to the current technical conditions, it is still impossible to achieve blockchain technology with "high efficiency and low energy", "decentralization" and "security". However, if one or several of its requirements are compromised, the resulting new technology set may be more attractive to practical applications because it is more in line with actual needs.

None of the existing blockchain infrastructure can solve the "impossible triangle". ETHEREUM has attributes of "decentralization" and "security", but it cannot meet "high efficiency and low energy"; EOS strives for its efficiency improvement space at the cost of "decentralization".

These infrastructures have a common limitation: their sub-chains inherit their "triangle" attribute, causing users to divert. For example, user A requires strong "decentralization", so they will select ETHEREUM; user B requires "high efficiency and low energy", so they will select EOS technology.

In order to solve these problems, Luther will build a modular blockchain infrastructure. Sub-chain builders are free to choose the modules for assembly, and each sub-chain builder has a different focus in the impossible triangle. They can flexibly select according to their own business characteristics.
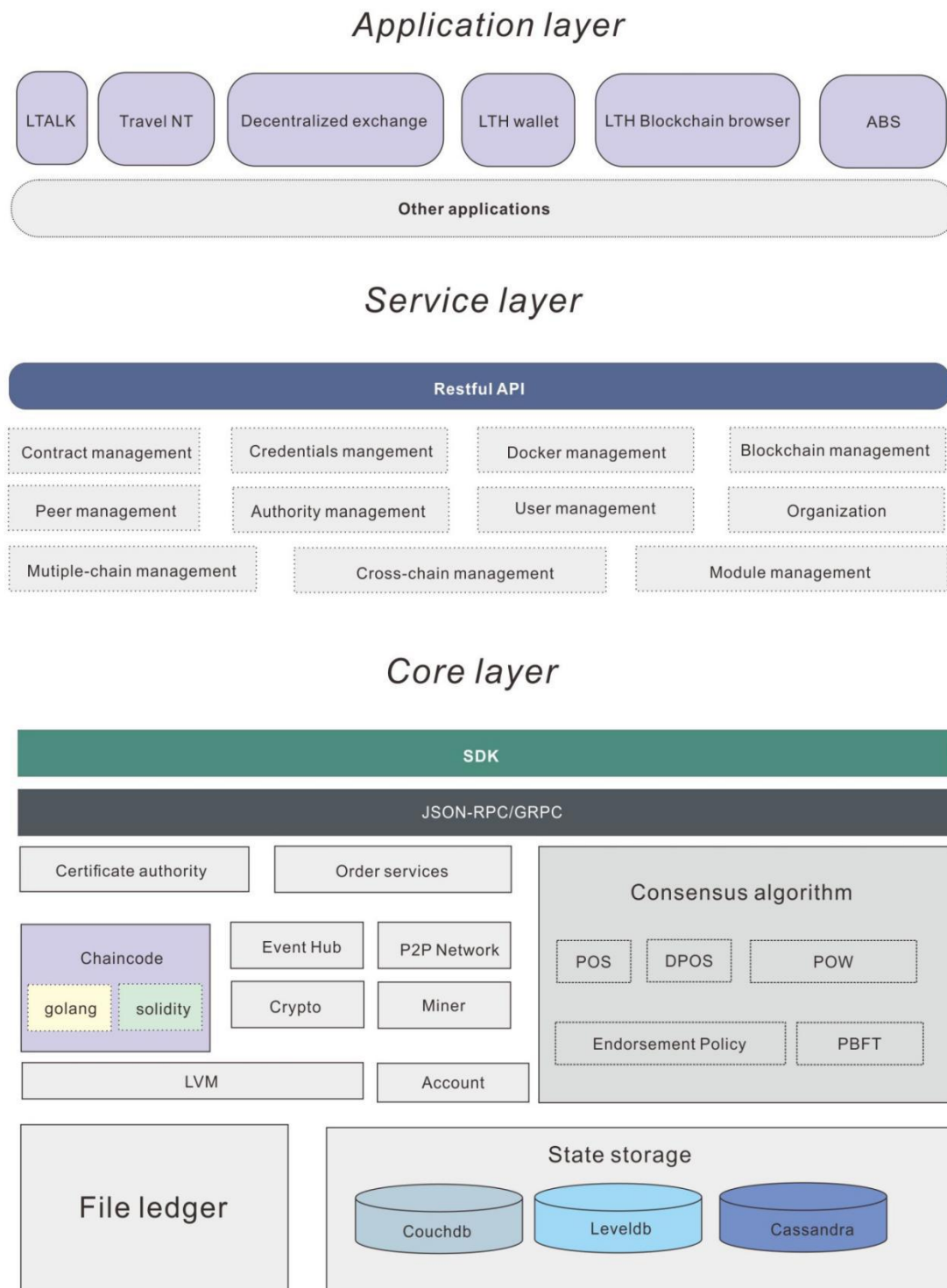
IV. Luther Technology Design

Based on the existing blockchain technology, Luther performs deep reconstruction and optimization, integrates Bitcoin, ethereum, bts graphene and other

technological advantages, and develops our own basic chains characterized by high performance, expansibility and modularization, so as to meet differentiated requirements in different business scenarios.

1. Overall Architecture

Application layer

| LTALK | Travel NT | Decentralized exchange | LTH wallet | LTH Blockchain browser | ABS |

Other applications

Service layer

Restful API

| Contract management | Credentials mangement | Docker management | Blockchain management |

| Peer management | Authority management | User management | Organization |

| Mutiple-chain management | Cross-chain management | Module management |

Core layer

SDK

JSON-RPC/GRPC

| Certificate authority | Order services |

Consensus algorithm

Chaincode

golang   solidity

| Event Hub | P2P Network |

| Crypto | Miner |

| POS | DPOS | POW |

| Endorsement Policy | PBFT |

| LVM | Account |

File ledger

State storage

| Couchdb | Leveldb | Cassandra |

## 2.   **Modularization of Components**

Luther modularizes all the cores of the blockchain, and in particular modularizes the consensus algorithms and provides services with Luther standard interface. As a result, Luther's sub-chain developers are able to flexibly choose the modular blocks, so as to build their own public blockchains, consortium blockchainss and private blockchains.
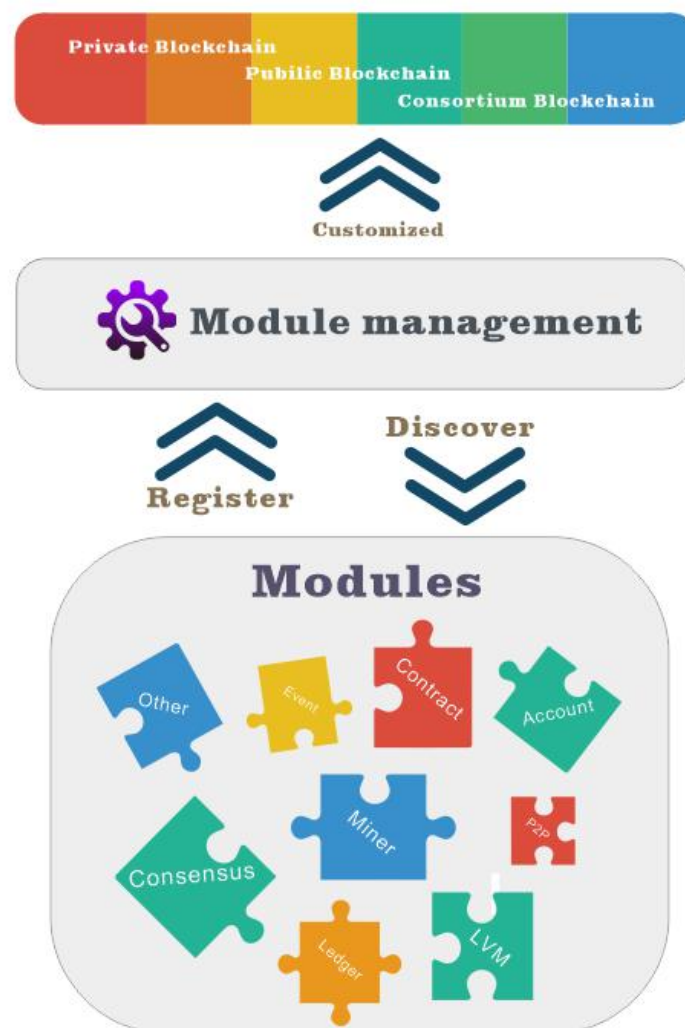
3. Improved Smart Contracts

According to the latest data, the number of DAPPs in Ethereum has reached 561. In order to ensure that DAPP on Ethereum can be migrated to Luther, LVM is perfectly compatible with the solidity smart contract.

In addition, Luther adds support for golang language development business smart contract. After being deployed on the blockchain, they provide services externally through a standard GPRC interface that encapsulates smart contracts for business processing.
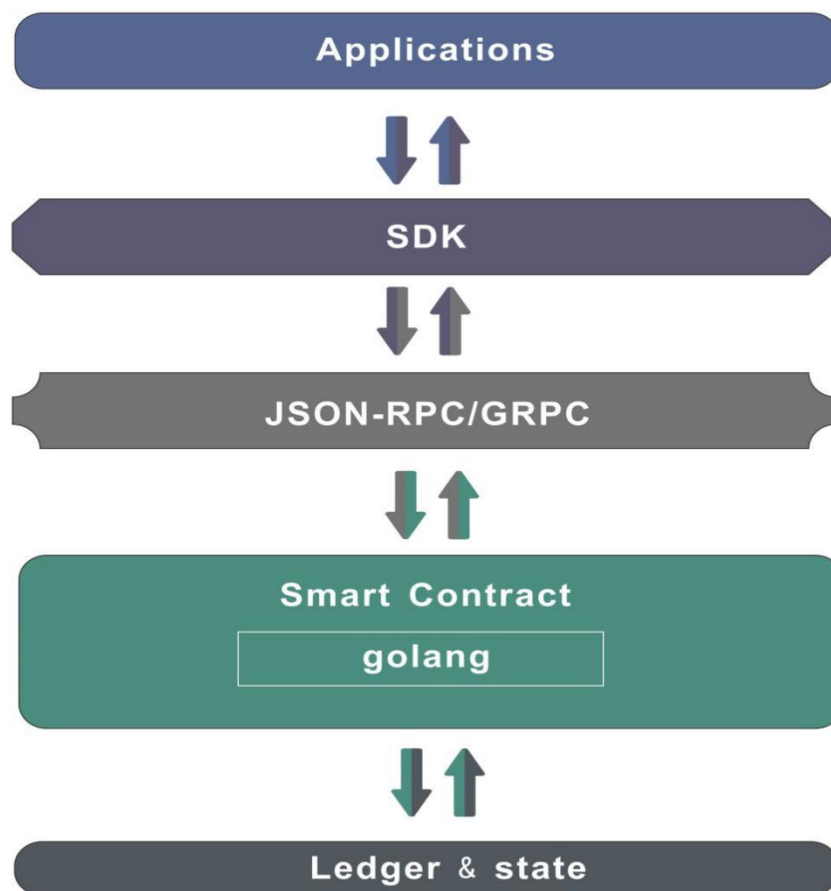
4. Expandable Storage

We make storage a pluggable component, which makes storage easy to expand; the cluster nosql database can be expanded easily so as to support the application of the huge data volume; leveldb, couchdb and cassandra are supported.
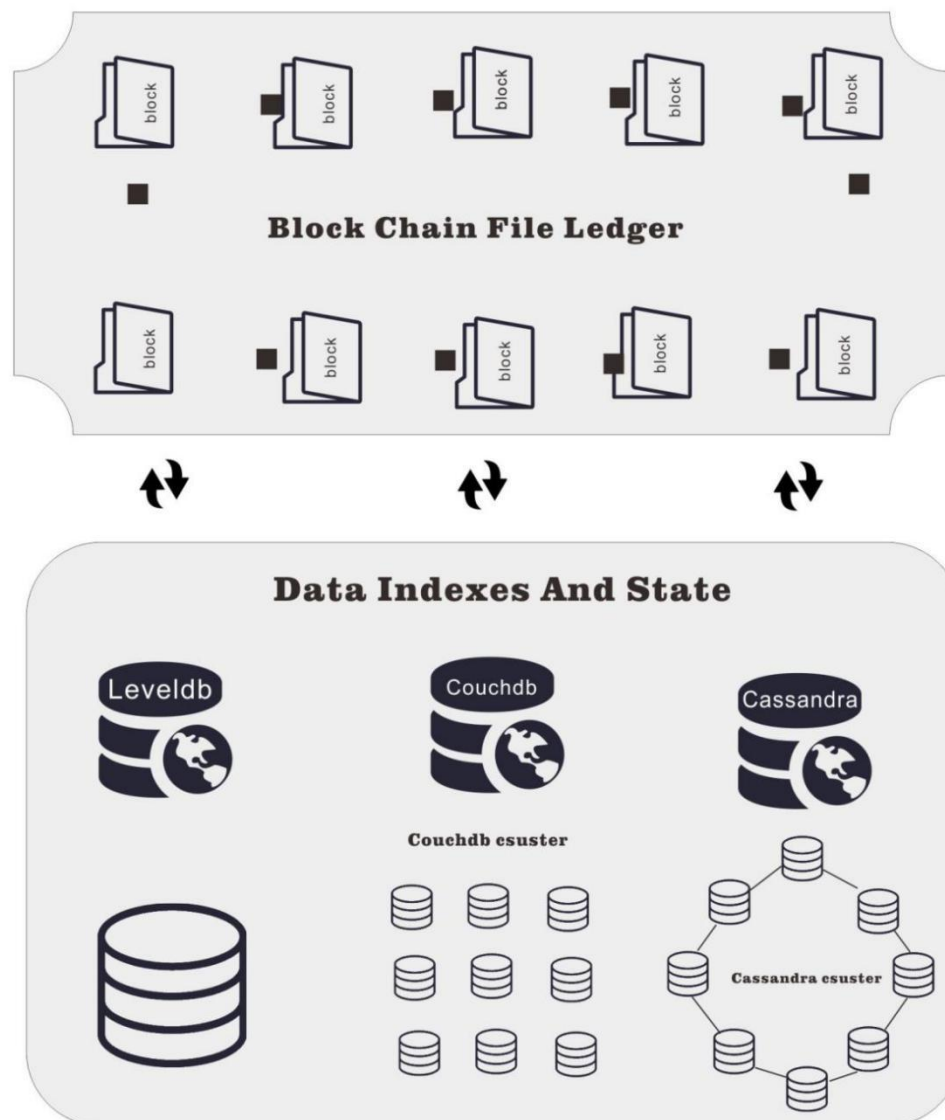

5. Multiple-chain Parallelism

A multiple-chain is a sub-chain in which multiple parallel operations are possible

in addition to the main-chain. Peers may join in sub-chains of different organizations alliances. The peers and sub-chains are in a many-to-many relationship. Each sub-chain has its own data access to achieve multiple-chain data isolation. As a result, this can meet the enterprises' building of consortium blockchainss.

A multiple-chain parallel application scenario is illustrated by a financial service scenario:
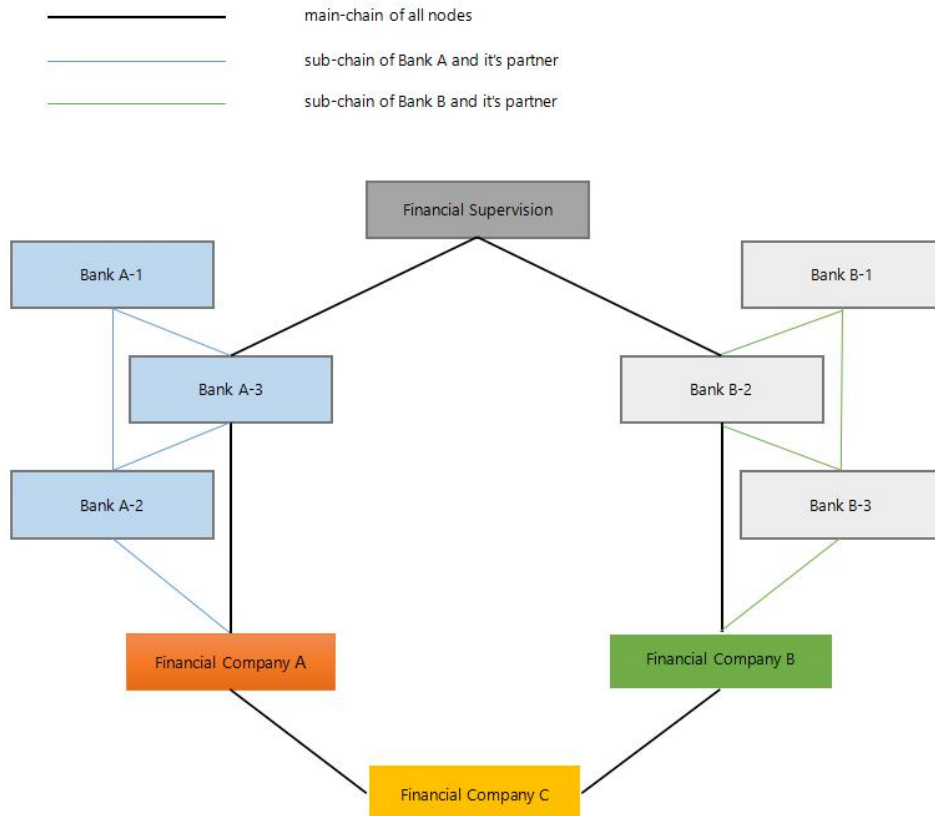
1. In this scenario, the blockchain' participating roles can be divided into banks, financial service providers, and regulatory authorities; all of them participate in the main-chain for data sharing and transaction consensus.

2. However, there may be competitive relationships among the participants in the roles, and there is a need for data privacy. Therefore, a sub-chain can be established between branches of the same bank. If other nodes are permitted by the sub-chain, they can also dynamically join this sub-chain for data sharing.

3. Through the design of main-chain and sub-chain, each participating role may not only perform ledger sharing and transaction consensus through the blockchain, but also perform permission control and core data isolation; so that all parties have access

to the data rights protection, sharing only the data that each role wants to share; the core competitiveness of the company can be maintained for data interconnectivity and win-win situation.

4. Taking ethereum as an example, anyone can participate in the blockchain. As a full-ledger node, the node owns all the data of the entire blockchain and is arbitrarily readable. Therefore, sensitive private data and confidential data cannot be stored.

5. Luther's data permission control is also modular, so users may choose according to their business needs.

6.　Cross-chain Protocol

Cross-chain, as the name suggests, uses a technology that allows value to flow directly across obstacles between chains and chains.

Blockchain is a kind of distributed general ledger. A blockchain is a separate Ledger. Two different chains are two different independent ledgers, and there is no correlation between two ledgers. It is essentially impossible to transfer value between ledgers, but for a specific user, the value that a user stores on one blockchain may turn into the value on another chain, which is the circulation of value.

If the consensus mechanism is the soul of the blockchain, cross-chain technology is the key to implement the value network for the blockchain and especially for consortium blockchainss and private blockchains. It is a good medicine to save the consortium blockchains from scattered isolated islands as well as a bridge for the external expansion and connection of the blockchain.

Due to LutherChain's modularity and multiple-chain parallelism, a large number of public blockchains, consortium blockchainss, and private blockchains will be implemented based on LutherChain technology. Therefore, if the cross-chain protocol module is built in LutherChain, developers may easily open the multiple-chain ecosystem through the use of cross--chain protocol.

1.   Luther cross-chain protocol plan to support bitcoin, ethereum, eos, luther sub-chain and so on.
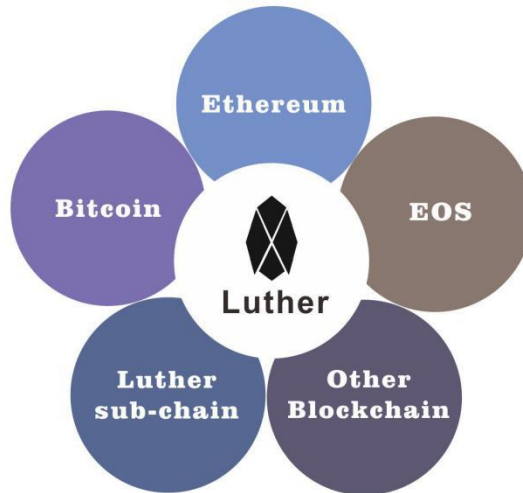
2.   The flow of cross chain between ethereum and LutherChain.
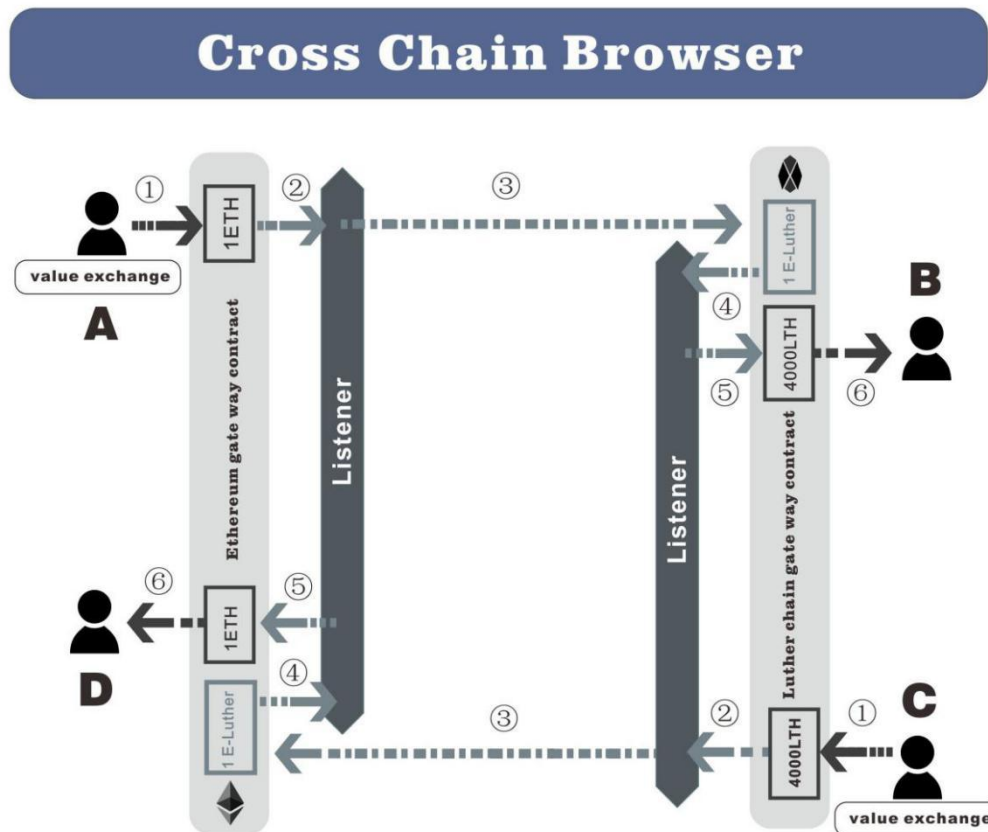
- Issue token E-luther on ethereum and token L-ether on LutherChain.
- Deploy gateway contract on both ethereum and LutherChain.
- Install transaction and block listener both on ethereum and LutherChain.
- Step①，Ethereum user A make a transaction with 1 ETH，the token value will be

exchange to the target blockchain's asset:4000 LTH base on real-time trading price，then invoke ethereum gateway contract to do transfer，the contract method includes：ETH amount，target asset LTH amount，target chain user B's address and so on.

● Step②，The transaction in step① been listened.

● Step③， A method of LutherChain gateway contract been automatic triggered by the Listener module，1 L-ether sent from Listener address to the pool address in LutherChain gateway contract,and the real ETH been kept in Ethereum gateway contract as reserve funds。

● Step④，The 1 L-ether transaction been listened by the Listener。

● Step ⑤， LutherChain gateway contract method been automatic triggered by Listener.

● Step⑥，4000 LTH been sent to address of user B.then the cross chain transaction done.

● Transaction from LutherChain to ethereum is the same as above.

● The whole life cycle can be monitor by cross chain browser.

7. Consensus Mechanism

POW

   The standard POW algorithm is provided as a module component. CPU and GPU mining are supported.

POS/DPOS

   The standard POS/DPOS algorithm is provided as a module component.

   POS: Also known as the equity certificate, it is similar to the property stored in the bank. This model will allocate the corresponding interest based on the amount and time of the digital currency held.

In simple terms, it is a system of allocating interest based on the amount and time of money held. There is a noun named token age in the POS mode. Each token generates 1 token age per day. For example, if you hold 100 tokens for a total of 30 days, then your token age is 3000. At this time, if you find a POS block, your token age will be cleared to zero. Every time 365 token ages are cleared, you'll receive interest of 0.05

tokens (assuming that interest is understood as 5% per annum). In this case, interest = 3000 * 5% / 365 = 0.41 tokens. This is very interesting. You can get interests on the holding tokens.

BitShares' DPOS mechanism. Its principle is to make each BitShares holder vote, resulting in 101 representatives. We can understand it as 101 super nodes or mining pools, and the 101 super nodes have the completely equal rights. From a certain perspective, DPOS is somewhat like a parliamentary system or National People's Congress. If representatives fail to perform their duties (when it's their turn, they are unable to generate blocks) they will be removed, and the network will elect new super nodes to replace them.

PBFT

The standard PBFT algorithm is provided as a module component.

PBFT: Practical Byzantine Fault Tolerance is a state machine replica replication algorithm. In other words, the service is modeled as a state machine, and the state machine replicates at different nodes of the distributed system. Each replica of the state machine saves the state of the service and also implements the service operation. The set of all replicas are represented by a capital letter R, and each replica is represented by an integer ranging from 0 to $|R|-1$. For convenience of description, it is assumed that $|R|=3f+1$, where f is the maximum number of replicas that may fail. Although there may be more than $3f+1$ copies, the additional replicas do not improve reliability other than reducing performance.

As the number of nodes increases, the performance of PBFT will decrease, and the number of public blockchain nodes is mostly large. Therefore, PBFT is used as a component for the consortium blockchains. As an enterprise-level consortium blockchains, PBFT has unique advantages.
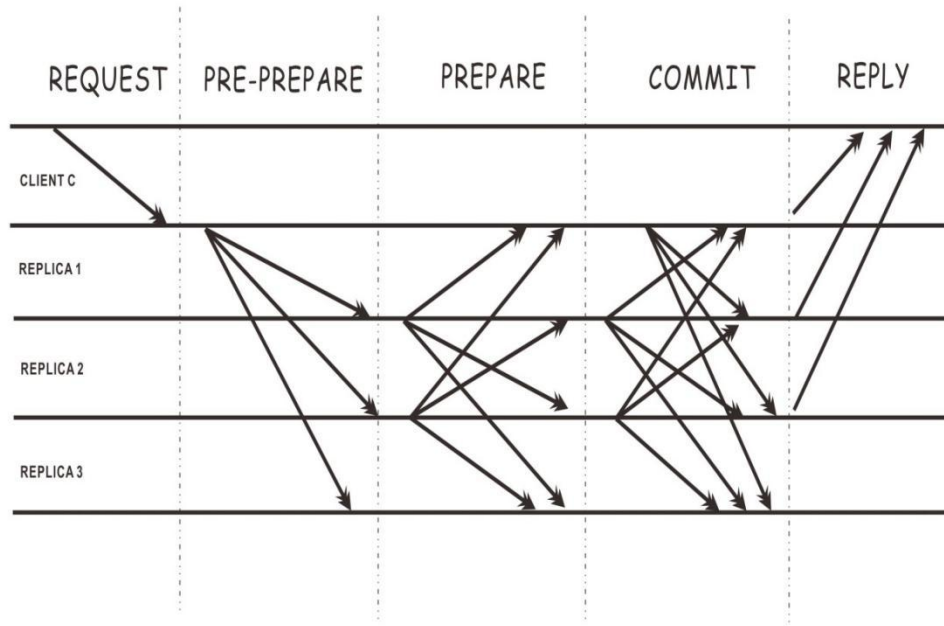
Endorsement Strategy

Like PBFT, the endorsement strategy model is used as an consortium blockchains consensus option. The endorsement strategy of the user-defined standard format is released along with the smart contract to the blockchain network. The endorsement strategy is flexibly configured according to the organization structure in the chain.

Example:

In a merchant alliance, merchant A has 20 nodes, merchant B 30 nodes, merchant C 40 nodes, and merchant D 50 nodes, together they form a chain;

Endorsement strategy is defined as:

(18 of A & 20 of B & 10 of C & 1 of D) or (15 of A & 22 of B & 38 of C & 40 of D)

For a transaction, each node executes smart contract, and the results are subject to an endorsement signature. In the endorsement strategy verification module, as long as the number of nodes described by the endorsement strategy formula has been verified, the consensus is then reached and the transaction is deemed to be valid; otherwise it is determined to be a failed transaction.
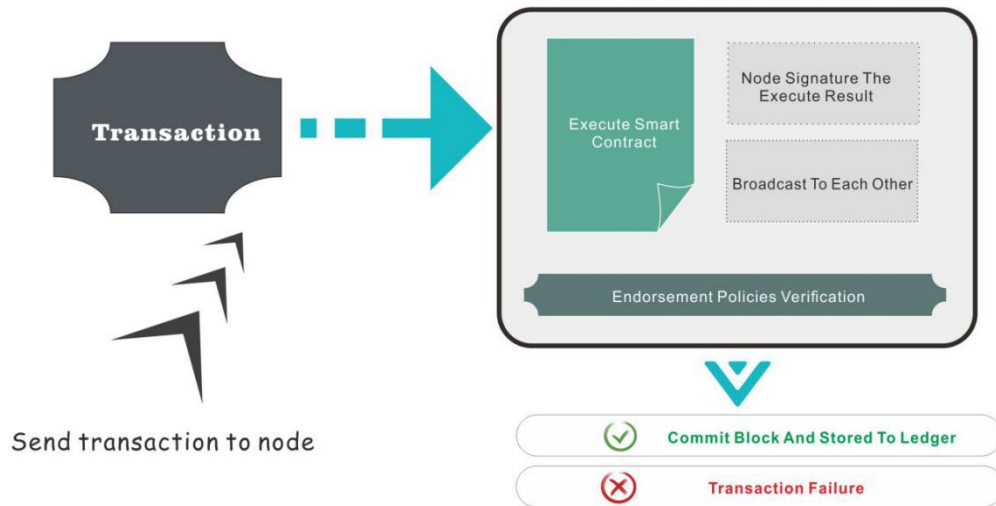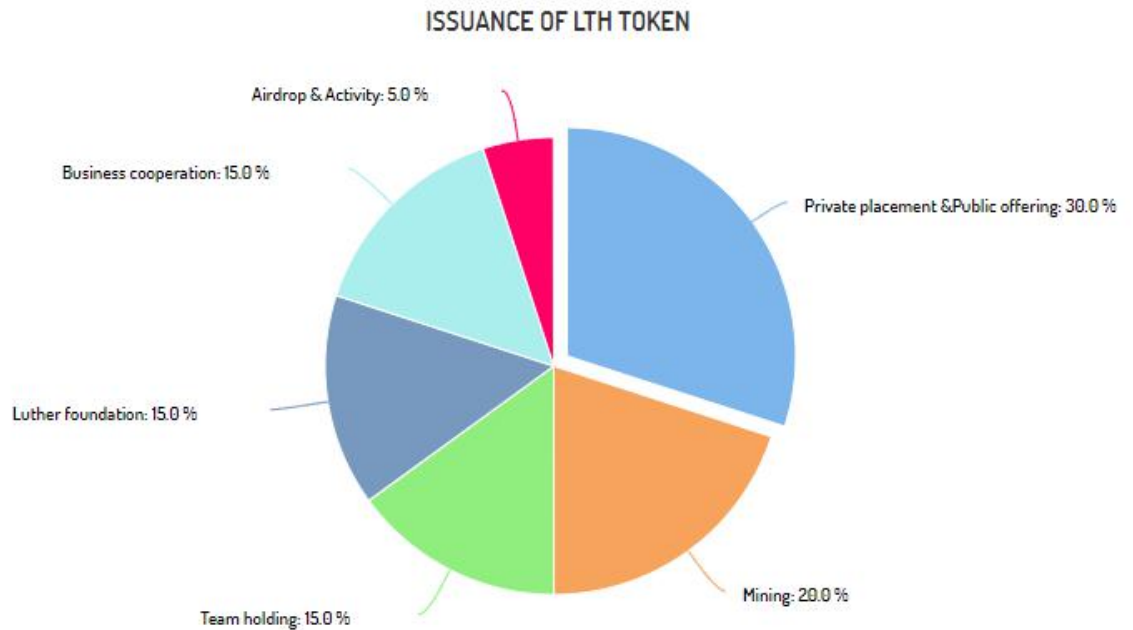
The weight of endorsement strategy is determined after the alliance is formed by free consultation among the members of the alliance.

V. Luther's Economic Model

In the Luther system, the system's built-in token code is LTH. The system's built-in token is the driving force of the entire system ecology, which will be used to support application development, pay the application consumption costs, support the exchange of sub-chain digital assets, participate in consensus rewards, and pay transaction fees.

(I) Issuance of Token

LTH was initially issued with 1 billion, which is divided into four major parts. The specific proportions are as follows:

ISSUANCE OF LTH TOKEN

Airdrop & Activity: 5.0 %

Business cooperation: 15.0 %

Luther foundation: 15.0 %

Team holding: 15.0 %

Private placement &Public offering: 30.0 %

Mining: 20.0 %

1. Private placement &Public offering, accounting for 30%.

2. Mining, accounting for 20%, this part was locked until LutherChain main net launch.

3. Team holding, accounting for 15%, this part was locked initially, which was unlocked linearly by installments of 20 months after being put online and unlocked 5% per month.

4. Injecting into community funds, accounting for 15%, this part will be used for the construction of community ecology;

5. Business cooperation, accounting for 15%, this part will be used for business cooperation.

6.Airdrop & Activity

(II) Blockchain Network Maintenance

Same as BTC, the total amount of LTH is constant and will not be inflationary.
20% of the total amount of tokens will be mined and halved every 2 years.

(III) LTH Value Embodiment

1. LTH token is taken as a fuel for transacting on the chain.
2. Due to deployment and execution of the smart contract, a certain amount of LTH will be consumed.
3. In the future, any Luther sub-chain assets will have a certain percentage of

airdrops on LTH token holders.

4. 30% dividends on all blockchain application revenues of Luther Foundation might be enjoyed. Dividends are issued pro rate based on LTH holdings.

5. Luther has many in Luther foundation first cooperative project Ltalk.

VI. Luther Development Roadmap

1. 2018 Q1

Ltalk, the first social and information sharing platform in the global blockchain industry, was designed.

The Luther main chain technology design was started

2. 2018 Q2

Ethereum's ERC20 token LTH was issued, and was replaced after Luther's main network launch.

Ltalk R&D was completed, and the beta version was issued.

Resources were docked.

3. 2018 Q3

Ltalk official version will be released on android and ios application market.
The marketing department will conduct the application promotion.
The communities such as Chinese ,English,Russia and Korea will be built.
LTH will be put online to three well-known overseas exchanges.

4. 2018 Q4

Luther main net R&D work will be fully implemented.
The layout of the Luther ecosystem will be carried out.
Luther will continue to promote ltalk, maintain rapid continuous iteration,
Expand the community scale.
LTH will launch to more mainstream exchanges to increase liquidity.

5. 2019 Q2
The main chain's beta version will be issued for testing by the number one player in the community.
LTH will launch to more mainstream exchanges to increase liquidity.
Luther ecosystem will be established.

6. 2019 Q3

Luther main net launch and LTH token will be replaced with real LTH.
The blockchain browser will be released.
LTH will launch to more mainstream exchanges to increase liquidity.
The roadmap and strategic direction for the next stage of development will be announced.
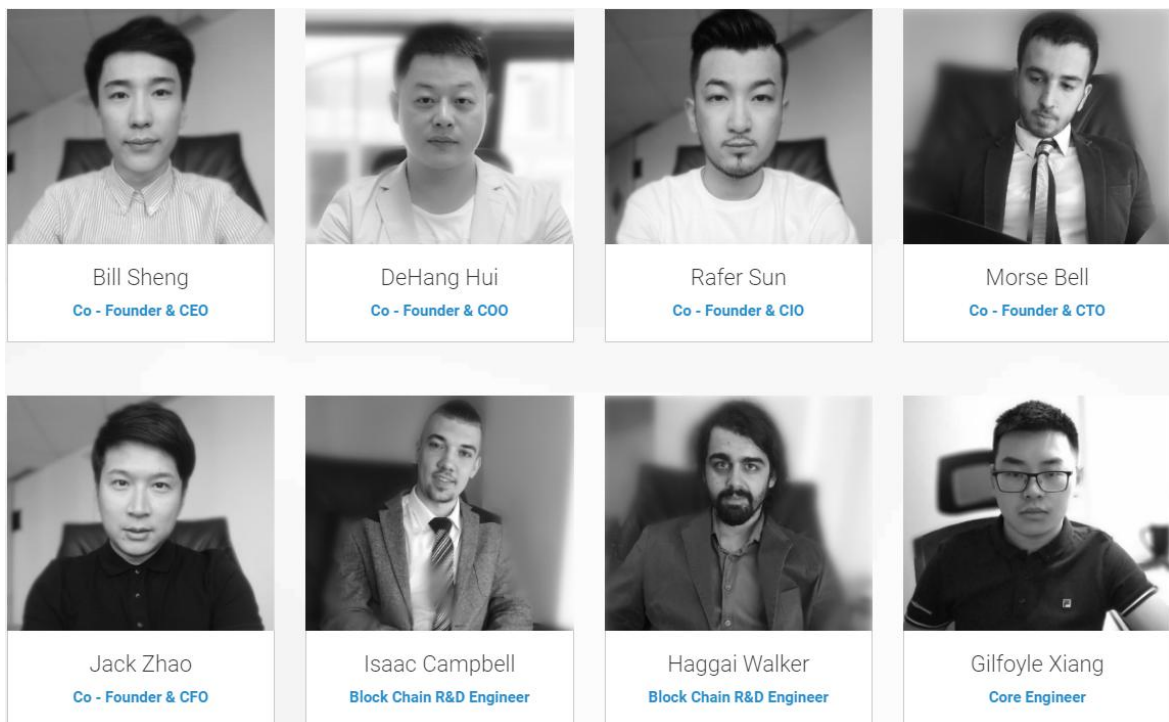
7. 2019 Q4

The Luther Foundation will set up a special fund to support applications on the LutherChain, Dapp, and subchains based on LutherChain technology.
Several Luther ecosystem projects will be continuously announced and supported.
LTH will launch to more mainstream exchanges to increase liquidity.

8. 2019

At the end of 2019, we plan to develop ltalk into a global blockchain ecological app for more than ten millions of users; to develop and support more than 100 Dapps on LutherChain, and to develop more than 20 LutherChain sub-chain projects.

VII. Team

Bill Sheng
Co - Founder & CEO

DeHang Hui
Co - Founder & COO

Rafer Sun
Co - Founder & CIO

Morse Bell
Co - Founder & CTO

Jack Zhao
Co - Founder & CFO

Isaac Campbell
Block Chain R&D Engineer

Haggai Walker
Block Chain R&D Engineer

Gilfoyle Xiang
Core Engineer

Watt Eddy **R&D Engineer**	Keppel Rodney **R&D Engineer**	Myrna shelley **R&D Engineer**	Tyler Gregory **R&D Engineer**
Joanna Percy **Art Engineer**	Bartholomew Joyce **Art Engineer**	Connor Garcia **Operations Manager**	Joan Lewis **Operations Manager**
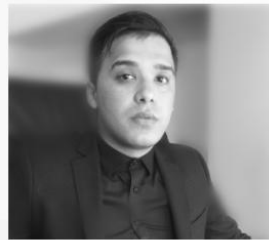
VIII. Conclusion

The team will drive the implementation of blockchain technology and the birth of unicorn application with practicality and innovation, and lead the fourth industrial revolution.

Luther Official Website: lth.one