

LEMO

White Paper v2.2 English



LEMO

Cross-application ecosystem for business data circulation, based on secure multi-party computation.

Offering application developers and operators a universal user account system, smart contracts, as well as ownership authentication and circulation of digital assets to build a flourishing decentralized data ecosystem.



IMPORTANT DISCLAIMER

There are risks, and uncertainties associated with Lemo and/or the Distributor and their respective businesses and operations, the LEMO tokens, the Lemo Initial Token Pre-sale and the Lemo Wallet (each as referred to in this Whitepaper). You can find a description of the risk related to the Token Pre-sale under the section Legal, which should be read carefully.

This Whitepaper, any part thereof and any copy thereof must not be taken or transmitted to any country where distribution or dissemination of Token Pre-sale or Initial Coin Offering like the one described in this Whitepaper is prohibited or restricted.

The LEMO tokens are not intended to constitute securities in any jurisdiction. LEMO tokens are utility token and cannot have a performance or a particular value outside the Lemo Platform. Therefore, this Whitepaper cannot constitute a prospectus or offer document for investment in securities.

This Whitepaper does not constitute or form part of any opinion on any advice to sell, or any solicitation of any offer by Lemo to purchase any LEMO tokens or give any help in any investment decision.

You are not eligible, and you are not to purchase any LEMO tokens in the Lemo Token Pre-sale (as referred to in this Whitepaper) if you are a citizen, resident (tax or otherwise) or green card holder of the United States of America or a resident of the People's Republic of China.

Contents

LEMO	2
IMPORTANT DISCLAIMER	3
Contents	4
Executive Summary	6
Lemo’s design concept	8
Why did we create Lemo	8
Components of LemoChain’s Ecosystem	15
Systems Architecture	17
Consensus Mechanism	18
Throughput	21
Data Storage.....	24
Safe Transactions	26
Smart Contract.....	28
Application Layer Services.....	31
Account System	31
Online Safe	32
Data Exchange Template	33
Lemo Wallet	35
Application Prospects Based on LemoChain.....	36
Multiple industry support	36
Application scenario	37
Lemo Release	40
Creation of Tokens	40
Lemo’s Pre-sale Plan	41
Overview	42
Early Investors.....	42

LemoChain’s Governance Ecological Framework.....	47
Lemo Foundation LTD.....	48
LemoChain Founding Team	50
Current team core member	50
Lemo Advisory Team	51
Lemo’s strategic partners	52
Lemo’s execution and iteration	53
Timeline	53
Lemo Pre–sale plan.....	54
Lemo iterative planning	55
The iteration of the LemoChain infrastructure	55
Business application iteration	56
Lemo’s Disclaimer and Risk Statement	57
Risk statement	58

Executive Summary

The Founders of LemoChain (Lemo for short) are committed to developing a decentralized data circulation ecosystem, focused on facilitating the effective open exchange of structured business data. Built on blockchain technology, Lemo's 'Smart-Contract Value Transfer Protocol' is able to achieve a P2P and B2B data exchange across a DApp platform – a decentralized application platform suitable for a range of industries (including education, social networking, gaming, recruitment, finance etc.). Lemo's innovative technology, comprehensive ecosystem governance and inclusive nature will facilitate an all-encompassing platform for widespread data pioneering. From a technical viewpoint, Lemo possesses strong research and development capabilities. Through implementing an established technological framework, Lemo will be the first blockchain to run on a D-PoVP (Delegated Proof of Valued Participation) consensus mechanism. This innovative mechanism will be implemented in alignment with varying regulatory requirements across a broad spectrum of commercial applications.

Meanwhile, the adoption of secure multi-party computation, zero-knowledge proofs and homomorphic encryption will ensure secure and efficient data transfer; thus establishing the underlying trust foundations for data circulation on Lemo.

From an angle of ecosystem governance, The Lemo Foundation is designed to drive R&D growth, governance transparency and the overall development of the LemoChain ecosystem, so as to strive for universal security and cooperation between all stakeholders. The Foundation regularly evaluates all aspects of the open source community from several dimensions such as code management, team management, financial management and public relations. Thus, the sustainability of Lemo, the efficiency of the Foundation's management and the security of crowdfunding can be ensured.

In regards to mobile applications, Lemo, along with service providers, will enhance business' off-chain capabilities by facilitating decentralized application development and providing smart contracts which align with real commercial logic. Eventually, not only does Lemo strive for the broad adoption of 'Go-Mobile' strategies; but ultimately aims to optimize traditional businesses using blockchain technology. Lemo maintains the belief that by realizing blockchain's potential for business development, companies can bring tangible benefits to a range of stakeholders.

Within the whole ecosystem, Lemo will collaborate with third-party developers to provide support and technical framework assistance, including:

- **LEMO Token** – The encrypted Lemo token (LEMO) will be the universal medium of exchange on Lemo. LEMO will be a stable store of value that will facilitate data exchange, regardless of time or location.
- **Commercial data matching and trading system** – Providing data distribution services based on multi-party computation calculations; assisting different applications in developing compliant and transparent data distribution channels.
- **Data Circulation** – Sharing of data (serving for all social apps), helping different apps to build legal and transparent data flow channels.
- **Account System** – One account has access to all apps, increasing conversion rates and expanding traffic sources.
- **Digital Asset Smart Contract** – Ensuring the ownership authentication of digital assets for developers and users; helping the circulation and liquidation of digital assets, thus improving user's mobilization.
- **Integrity System** – User credit system; an interest-driven system, evaluating overall ecosystem contribution; so as to recognize and reward positive contribution whilst discouraging negative input. This will aid developers in selecting target users whilst increasing conversion rates.
- **Data encryption storage and transmission system** – Providing a securely encrypted system for the storage and transmission of data for B-end users and developers .

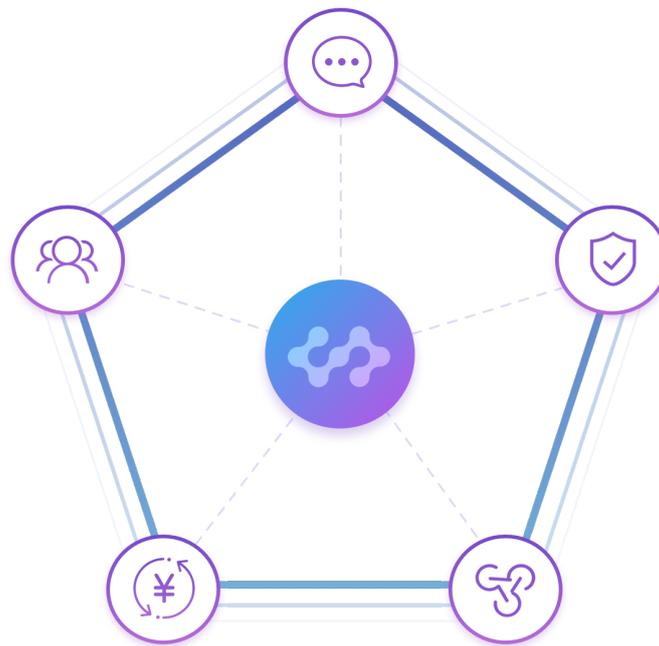
At the same time, we will lay down a reward plan to encourage early third-party developers to work with us on LemoChain-based mobile-end services, promoting the efficient and synergetic development of blockchain.

Lemo's design concept

Why did we create Lemo

Since Bitcoin's implementation of open source P2P currency in 2009, we have witnessed a global phenomenon: an emergence of countless projects founded on achieving socio-economic development by means of decentralization and distributed ledger technologies. Arguably, the most notable of these projects being the Ethereum project, which focused on proving the potential of smart contracts whilst developing a universal platform for decentralized applications (DApps). However, despite these advances, the blockchain world still faces a host of challenges from both technical and industrial perspectives:

- Many existing smart-contract platforms have struggled to connect with real business logic due to the technological distance from everyday business, with both Bitcoin and Ethereum architecture having limited widespread application to the common consumer.
- Current consensus mechanisms lack flexibility and efficiency; the exchange of value is not centered around transferability to real commercial scenarios.
- The compatibility problems between different blockchain platforms. For example, UTXO-based Bitcoin ecosystem isn't compatible with Account-based Ethereum.
- Existing blockchain platforms are isolated from off-chain data. At present, most smart contracts solely accept on-chain data as the trigger condition, lacking interchangeability within the real world.



We are committed to building a brand–new blockchain data transmission ecosystem; Lemo, as a universal Internet data value transmission protocol for future decentralized applications, digitizing and tokenizing data values, and promoting Blockchain technology is applied to real–life business scenarios.

We are aiming to build a new data circulation system, based on LemoChain, which will become the universal online data transfer protocol. This is how LemoChain will connect blockchain technology with the real world.

At the same time, in offline and online business activities, valid data transfer and exchange has always been the power source of their business model. Traditional commercial activity faces the following obstacles whilst obtaining this data:



as well as:

- Data transmission security
- The use and attribution of data are not effectively guaranteed and the process cannot be monitored and opaque
- The trust costs of both sides of data transactions are generally high, which directly leads to the liquidity of the data, the value it generates, and its limited value.

The vision of LemoChain

LemoChain is the future data value transfer solution for applications and businesses alike. It is an ecosystem powered by blockchain technology. The Lemo Foundation is aiming to integrate blockchain technology into a range of industries, such as: social networks, gaming, education and recruitment. This will be executed through building communities of third-party developers, operating on a network that is constantly evolving alongside the ecosystem.

The design principles of LemoChain



Whilst striving to facilitate the optimum operation of Lemo-based applications, scalability must be of top priority. Slow transaction speeds inhibit the overall success of the ecosystem and prevent the growth of future applications; essentially rendering the underlying vision of a flourishing decentralized ecosystem on Lemo as flawed. For example, CryptoKitties caused 20,000 transactions on the Ethereum network to be blocked, whilst consuming 15% of the entire network. The DPoS based graphene/EOS framework can provide 10,000 TPS with an average transaction speed of 1 second; thus, reaching Visa scale transaction processing capabilities. These are hugely promising developments but has highlighted some clear room for development to Lemo.

Lemo will address the following characteristics in its' technical design:

1. Universally Applicable

As a data circulation blockchain focused on a broad market, Lemo serves no specific industry and strives for widespread integration both within and between industries. Meanwhile, Lemo will provide development kits and tools to aid developers' integration into the ecosystem.

2. Easily Upgradable

Bugs are an inevitable hurdle for any project and regular optimization is key to long term success of any organization. Bitcoin's centralized computing power has resulted in a mining pool with no democratic input; It's evolution as a stable decentralized network is arguably hindered by the conflict of interest that occurs between all stakeholders, from users to miners and even between mining pools. Conversely, Ethereum's failure to reach a common consensus following the hack of the DAO led to the hard fork into ETH and ETC, thus creating two separate forks that both require their own regular bug fixes. Lemo will ensure full community input and decentralized contribution, whilst ensuring all bugs and shortcomings are met with a high degree of efficiency and transparency.

3. Security & Privacy

Lemo, from its core blockchain code to its upper application interface will coherently

safeguard user privacy across all aspects of data exchange within its' ecosystem. This will ensure sole ownership of data from the original holder, with no access available to any third party. All code related to the data privacy and user protection will be open-sourced entirely to accept consistent community feedback. Additionally, Lemo will organize regular code audits to ensure the entire mechanism can withstand any malicious attacks.

4. Transparency & Support

Lemo will develop blockchain infrastructure with a friendly user interface for true accessibility; with this being backed up by the release of development kits for developers wishing to operate on Lemo. Lemo will also be in regular collaboration and idea sharing with industry partners, aiming to align with one core vision of a prosperous open data exchange infrastructure.

In response to the current limitations and various issues with existing blockchain technology, Lemo has proposed the following goals targeted at addressing existing public blockchain platforms (Circa October 2017):

- To make blockchain universally compatible with real world business;
- To develop a flexible and comprehensive consensus mechanism;
- To lower the transaction cost and solve the existing credit problems in current business environments;
- To conditionally release the smart contract based on the on-chain data, achieving interconnection between blockchain and the real world;
- To provide a universal account system to eliminate boundaries faced by current applications;
- To protect the rights and interests of all participants;
- To aid the full circulation of participant's digital assets;

Based on all these goals, Lemo will provide a solution which mainly includes five major notions to improve the overall application data circulation in the future:

- 1. A data circulation system based on Secure Multi-party Computation, with smart contracts to aid users effectively exchange and circulate data and**

- digital assets;
2. A high-speed decentralized data storage and transmission system based on blockchain smart contracts and homomorphic encryption technology. This will help developers, service providers, and users securely store data (digital assets) to ensure that all participants rights and interests are rightfully protected.
 3. Issuing LEMO tokens as a quantitative proof of ownership and as a distribution medium for digital assets;
 4. An account system that establishes a common account for all participants in the system and eliminates the boundaries between varying businesses and applications on Lemo;
 5. A credit system that uses smart contracts to agree on the credit impact of 12 different community behaviors; maintaining the value system of the community in a decentralized manner whilst rewarding quality participants and discouraging and/or punishing negative contribution.



Whilst looking at security, the antagonistic relationship between developers and users, combined with the competition between different developers in the same field is hindering industry and societal progress. In Lemo's decentralized architecture, users and different developers are all participants with a common goal. By contributing their own products, development and operational capabilities, they each provide to the ecosystem: information, data, community governance, traffic, storage space, assets, etc., to receive tokens from the community. At the same time, Lemo provides a liquidation and circulation channel for digital assets and equity that will benefit all participants in the system.

Components of LemoChain's Ecosystem

Stakeholders

The stakeholders of LemoChain represent the true operational capability of LemoChain's ecosystem. Defining them from various dimensions, we've divided stakeholders into following categories:

1. Users

Users enter into the ecosystem via DApps; By creating accounts, inviting other users, and by positively contributing information users obtain financial reward, 'Lemo'. Also, Lemo can be used on other Dapps on LemoChain to pay for services such as data storage, or on cross-application data ownership authentication and circulation.

2. Developers/Carriers

Developers/Carriers enter into ecosystem through integrating and using Lemo API in their applications. By building applications, acquiring users, and contributing encrypted data, they gain Lemo reward. After ownership authentication and quotation conducted by Lemo, data contributed will have access to the overall circulation, so as to offer other participations the valuable information they need, through which developers can gain Lemo. Developers can also broadcast within LemoChain for their data demands (new user acquisition, business analytics and user behaviors). For those with limited app developing capabilities, LemoChain will also provide fundamental user framework so even those with less resources can reap the benefits of the Lemo ecosystem.

3. Storage nodes

Storage nodes enter into ecosystem by contributing their own storage space and computing power. Owners of limited storage server space can represent storage nodes

to join the ecosystem and get Lemo tokens by providing decentralized storage and computing power for the entire ecosystem.

4. Investors

Investors can acquire early ownership of Lemo Token in the pre-sale stage. Investors are early supporters and visionaries of the LemoChain ecosystem. The funds raised by investors will be used in developing LemoChain, community building, marketing promotion, and daily operation, whilst laying the foundations for other participants' benefits.

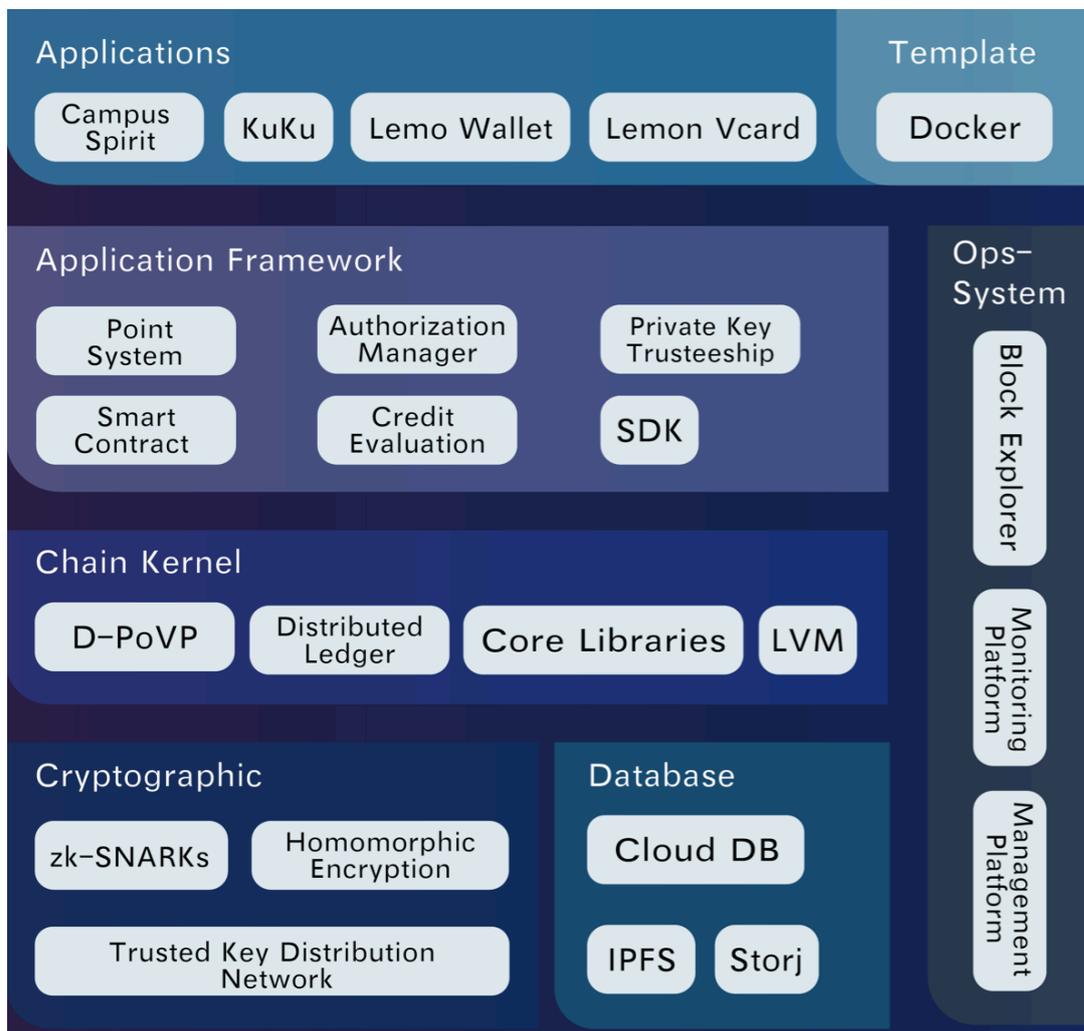
5. Opinion leaders

Every 12 months, Lemo Foundation LTD will nominate candidates of opinion leaders through comprehensive evaluation based on annual community contribution. Then, community participants vote by ballot. Opinion leaders can bring forward opinions on ecosystem development and then after auditing, the future trend of Lemo ecosystem will be determined by participants' voting. At the same time, opinion leaders also embrace voting rights in The Lemo Foundation, enabling them to work on LemoChain-related decisions, whilst gaining Lemo from the community for their valued contribution.



The Lemo ecosystem is open and free for everyone. People will be required to pay Lemo only when using specific storage or data. Lemo token can be acquired by investing in Lemo Foundation LTD during early stages or making contributions to the ecosystem including contributing their own data, creating traffic, providing storage and computing, inviting new users, participating in community governance and more.

Systems Architecture



Consensus Mechanism

The consensus mechanism has always been a hot topic in blockchain research. The prevailing view is that effective algorithms must comply with the Byzantine fault tolerance principle. And it needs to be safe, clear and irreversible in the shortest possible time, and it is easy to provide a most solid and decentralized system. In practice, the process is divided into two aspects: selecting a unique node to generate a block and making the transaction ledger irreversible.

The Byzantine fault-tolerance problem can be expressed as a major solution to the problem of a general trusted communication. A group of generals want to achieve a certain goal (consistent attack or retreat), and the individual actions cannot be completed. A consensus must be reached through cooperation. However, due to the presence of traitors, the generals do not know how to achieve agreement. Here "consistency" is the main content of the discussion of General Byzantine. Currently there are many algorithms that have solved the Byzantine General problem. Here are some common algorithms

1. PBFT

The PBFT mechanism is represented by the IBM HyperLedger fabric. The core of a solution it describes is the state machine replica replication algorithm. First, a master node is responsible for block production; then, the received transaction data is broadcast to the entire network. Eventually each node keeps a copy of the state of the service. The total number of sets composed of all copies is denoted by N , and each copy is represented by 0 to $|N|-1$, as long as the number of untrusted copies is (analogous to the number of traitors) $f \leq (|N|-1)/3$, then this system can operate normally. Under this mechanism, all nodes eventually reach the same consensus and therefore do not diverge. If the master node goes offline, the backup node triggers a timeout mechanism and selects the next master node based on the node number.

The working premise of PBFT is that the nodes in the network are known in advance, and therefore are only applicable to the consortium chain or private chain. Nodes working under the PBFT mechanism need to communicate with each other. The complexity of network communication is $O(n^2)$. The traffic volume will grow explosively as the number of nodes grows. In a public-chain environment, it will cause serious broadcast storms.

2. Proof of Work (PoW)

PoW is a research report posted by Nakamoto in a secret crypto-discussion group in 2008. The report describes his new ideas on cryptocurrency and the proposed bitcoin consensus algorithm. Each node in the entire system provides computing power for the entire system (abbreviation referred to as computational power). Through a competition mechanism, the nodes that have completed the most outstanding calculation work are rewarded by the system, once the distribution of newly generated currencies is completed. Simple and stable, it has withstood all kinds of attacks after attracting the attention of various hackers and scientists.

3. Proof of Stake (PoS)

The POS mechanism can be described as 'virtual mining'. Since PoW mainly depends on the scarcity of computer hardware to prevent witch attacks, PoS relies mainly on tokens in the blockchain itself. The holder holds the token as a deposit in the PoS mechanism so that they become validators. The PoS algorithm randomly selects one of these verifiers and gives them the right to generate the next block. The basis for selection is how much they invest in tokens and how long they hold tokens. If, within a certain period of time, the verifier does not produce a block, a verifier will be reselected instead of generating a new block. Similar to a system that distributes interest based on the amount and timing of token possession. The actual implementation of PoS will also have some mechanisms for clearing currency age, currency decay, etc. The PoS mechanism will have the advantage of not being able to carry out force attacks because the person who launches the attack needs to hold 51% of the total currency. After the attack causes the currency value to fall, he will be the person whose total currency value is most damaged.

Under the PoS mechanism, some holders will hold large amounts of tokens for a long period of time in order to increase voting weight. As a result, the total tokens in circulation will be reduced and prices will be more vulnerable to fluctuations. Because there may be a large number of big players or mine pools holding most tokens in the entire network, the entire network may become more and more centralized as the running time increases.

4. Delegate Proof of Stake (DPoS)

The DPoS consensus mechanism sacrifices certain aspects of decentralization on the basis of PoS, whilst greatly accelerating the time-consuming transaction confirmation process. The main principle is to randomly select a Lemo limited number of agent nodes among all nodes, and these nodes take turns accounting and take the consensus of the agent as the consensus of the entire network. New block rewards are shared by both agents and voters. In order to avoid adverse effects on the blockchain after the malicious node becomes the agent, the DPoS mechanism needs to re-elect the agent after a certain period of time. DPoS currently has the advantages of maturity and high throughput. Only the agent node can reach a consensus to confirm the transaction, and its transaction frequency can even reach the centralized Visa settlement scale.

5. Delegated Proof of Valuable Participation (DPoVP)

LemoChain integrated the BFT and DPoS consensus mechanism, and included the value of user contributions into the scope of incentives to develop a new DPoVP mechanism. The representative feature of this technology is to define multiple types, not just to acquire tokens in the mode of renting and selling idle computer resources, and to quantify the user's behavior through various dimensions of the scoring system, as a user's contribution to the platform, and loyalty. The measure of degree. On the one hand, it provides a standard for identifying high-quality users. On the other hand, it can also be used as a platform to motivate users. The platform contributes to the prosperity of each application ecology on LemoChain through rewards to users, and further attracts more traffic to the platform. This virtuous circle mechanism has become a major boost for LemoChain's rapid application development.

Throughput

The basis of the DPoVP consensus mechanism combines the advantages of BFT's fast consensus and the DPoS's throughput capability. It adopts the rule of out-of-sequence. Once the block from the last witness is received by the two-thirds node, it can be immediately confirmed. Start production of the next block. Equivalent to the block time interval is only limited by the network transmission speed, under normal circumstances can achieve less than 1s average verification speed and average 8000TPS data throughput.

2.1 Voting

In order to maintain the independence and scalability of functions, Lemo uses smart contracts to implement voting. The node is registered as a candidate through the contract and accepts user voting. Finally, the first 21 nodes are selected as witnesses based on the voting results.

2.2 The ownership of bookkeeping rights

The bookkeeping right mainly solves the problem of whether to block oneself or when to block. Witnesses proceed to block in the lexicographic order of the address. After you block out or receive a new block, you need to recalculate the countdown of your own block. After the time is zero, a new block will be generated directly.

First we define l to indicate the blocker number. Have:

- The current node's block number;
- The block number of the block that it produced or received and passed. Height is +1 of the current chain height;+1 ;
- The block number of the previously confirmed block before confirming the new block;

$$T = \begin{cases} t_w & , d(I_{me}, I_{receive}) = 1 \\ (d(I_{me}, I_{header}) - 1) * t_o & , d(I_{me}, I_{receive}) > 1 \\ T & , d(I_{receive}, I_{header}) < 0 \cup d(I_{receive}, I_{header}) > 1 \end{cases}$$

Define d as the distance of the two outlier numbers:

$$d(a, b) = ((I_a - I_b) + C) \text{ mod } C$$

Where C is the number of consensus nodes.

The validity of the new block needs to be verified before triggering the recalculation countdown. The countdown formula is as follows current time;

Timestamps received in the header of the block;

The waiting time for the current node to come out of the block. This is to prevent the block from going too fast, resulting in the early transactions being less empty;

The maximum available time for the block to come out of the block, beyond which the next node should immediately block out;

2.3 Block risk at the same time

Assume that the communication is normal at a certain moment, A node is out of the block, node B should be out of block at 10 seconds, and node C should be out of block at 20 seconds.

A quickly blocks and broadcasts, but fails to synchronize to Node B and synchronizes only to Node C. The C–node recalculated block time may be 10.3 seconds. This causes B and C nodes to block out in a very short period of time and broadcast to other witness nodes, resulting in a fork, unable to reach a two–thirds consensus.

According to the time calculation formula, the witness node does not recalculate (shorten) the block–out time when it receives discontinuous blocks, and it assists in broadcasting the confirmation information of other nodes. The nodes make decisions after trying to collect all the blocks on all branches.

The forking selection rule is to select the longest chain preferentially, and when the same length is selected, the lexicographic order of the block hash at the bifurcation is

preferentially selected to be the front chain.

$$A \leftarrow C \leftarrow D \leftarrow E > A \leftarrow B \leftarrow D > A \leftarrow C \leftarrow E$$

All nodes select the forked chain according to the same rule. After reaching two-thirds of the consensus, all the blocks in the chain enter the “final confirmation state” and are broadcast to ordinary nodes. Since bifurcation occurs at the consensus node, it does not have any effect on ordinary nodes that only receive access to the “final status” block.

2.4 Consensus Network Splitting Risk

Assume that 21 consensus nodes have 11 in China and 10 in the United States. Due to the special circumstances such as the interruption of the optical cable, the network is split into two parts that cannot communicate with each other, each of which generates a bifurcation chain. Here are two networks named C and A.

Each node will continue to count down and out of blocks, but it will never receive more than two-thirds of the node consensus. The witness no longer broadcasts blocks to ordinary nodes. Taking the C network as an example, in the case of ignoring block time and network transmission time-consuming, the time for each node to cycle (generate block) is linearly related to the number of A network nodes, , the average block interval is:

$$\frac{C_A \times t_o}{C_C}$$

Obviously, at the same time witnessing more nodes will produce more blocks. After the recovery of the optical cable, the witness network is connected and the new block can be broadcast to all nodes. Each node pulls the complete branch chain along the parent block hash, and selects the final chain according to the longest chain principle. Thus, two-thirds of the consensus reached in each block of the chain began to be broadcast to ordinary nodes. The process of confirming the block in this case will be stagnant for a while, but there is no security risk for the transaction on the chain.

Data Storage

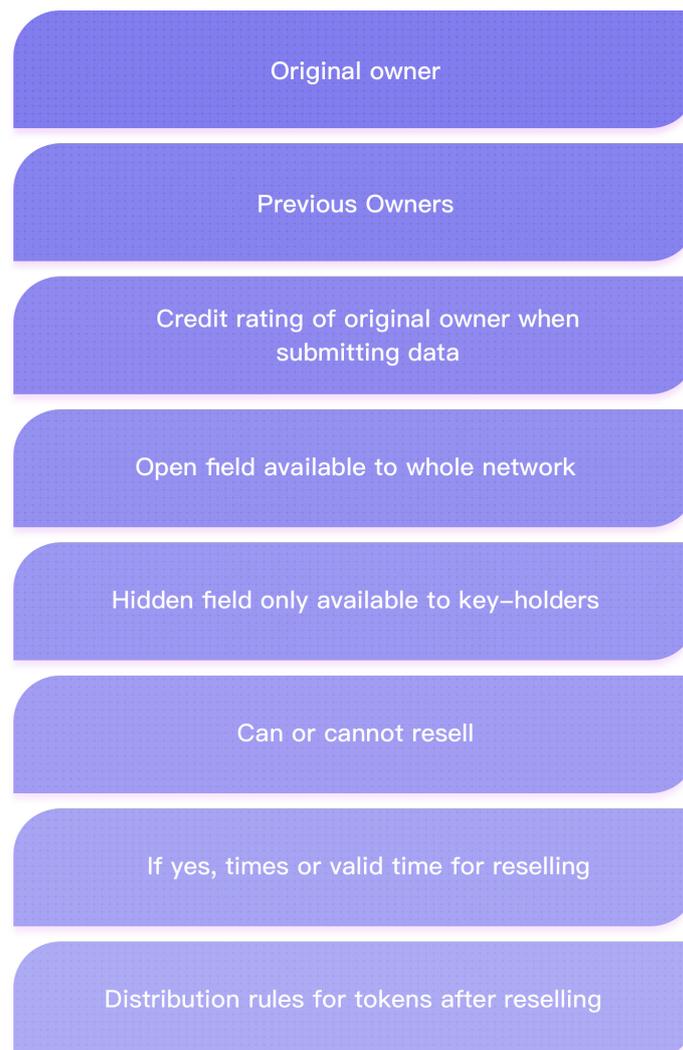
Lemo aims to create a decentralized data rights and circulation platform; the safe storage, encrypted transmission, and copyright attribution of participant data are crucial to the success of such a platform. The blockchain's security largely depends on it being mirrored by a large number of nodes and being 100% available. The storage of large, variable files on the chain will result in very high cost. For example, there is a high-performance blockchain application that processes 1 million transactions per second. Each transaction generates 100 bytes of records, and the consumed storage space will increase at more than 100MB/s. In order to maintain practicality, it is necessary to periodically truncate transaction records on the blockchain and save a blockchain state snapshot. However, the complete transaction record

will still be copied to each node, causing unnecessary backup overhead. Therefore, it is a practical and nonextensible decentralized file storage solution to store large-size data in the blockchain.

Flexible docking will support decentralized IPFS, storj file system, centralized cloud database and other programs, therefore providing users with a more diverse choice when it comes to data storage. In order to further simplify the application platform interfaces, Lemo will provide: a storage system adapter SDK, a public and private key generation package, address generation, signature verification, encryption, decryption and other functions. These will be shielded by complex signature generation rules, coding-conversion problems, and a variety of underlying error-code processing logic. The user identity management module and the private key storage module can be optionally introduced on the interface to reduce the public-private key management burden on the service application. Overall, Lemo is providing a convenient and easy to use interface for business developers.

IPFS is a global, P2P distributed version of the typical cloud system. It reduces the risk of data loss due to data center failures. IPFS's p2p network uses DHT technology, which replaces domain-based addresses with content-based addresses. IPFS is a global, P2P distributed version of the typical cloud system. It reduces the risk of data loss due to data center failures. IPFS's P2P network uses DHT technology, which replaces domain-based addresses with content-based addresses.

The centralized cloud database will be built on a world-class system of large scale cloud service providers, running as a stable, reliable, and low-cost database. It can provide 99.99999999% data reliability, 99.9% availability, up to 200gbps throughput and low latency to 1ms. Lemo will encrypt user data and open source code to secure a high-trust relationship and ensure that the privacy of user data is not violated.



Safe Transactions

In a traditional private data exchange scenario, the data of both parties in the transaction needs to be disclosed to each other or be matched by a trusted third party. In the current volatile and malicious business environment, this is extremely risky. The third party's right to facilitate the transaction is too large, and there is the possibility of leakage, tampering, and concealment of data between the two parties. As a result, protocols that can support joint computing and protect the privacy of participants have become increasingly more recognised. Lemo is committed to introducing Secure Multi-Party Computation (SMC) to solve this problem.

Secure multi-party computation is a collaborative computing solution that solves the problem of privacy protection among a group of non-trusted parties. SMC ensures the independence of input and the correctness of calculation; all without disclosing each input value to any of the participants. In general, a secure multi-party computing problem calculates any probability function based on any input to a distribution network. Each input party has an input on the distribution network. This distribution network needs to ensure the independence of the input and the correctness of the calculation. Also, in addition to their respective inputs, they do not disclose any other non-relevant information that can be used to derive other inputs and/or outputs.

Taking marriage and love website pairing as an example, the user's conditions and features are mapped into points in a t -dimensional space.

$$P = (x_1, x_2, \dots, x_t), x_i \in [0, 1]$$

Let the target of the demand side be a , the data of the data provider is to satisfy:

$$a, b_i \in P$$

The matchmaking transaction algorithm can be summarized as the nearest neighbor algorithm NN in the t -dimensional space b , that is, the minimum distance d between a and B is found to be minimum

$$b' = \text{NN}(a, B) = \min_{i=1, \dots, n} d(a, b_i)$$

In order to protect the confidentiality of the B data, the nodes in the blockchain need to be isolated from the data a and b , and only the encrypted data can be obtained. Therefore, Lemo introduced will introduce Fully Homomorphic Encryption to perform data matching calculations. Fully homomorphic encryption can perform arbitrarily complex operations on encrypted data without a decryption key to achieve secure plaintext computations.

Let the encryption algorithm be: $E(x)=c_x$

The decryption algorithm is: $D(x)=p_x$

Limited by the performance of the homomorphic encryption algorithm, LemoChain chooses the square of the Euclidean distance to calculate the matching degree. The optimal match calculation formula is:

$$b' = \text{NN}(a, B) = D\left(\min_{i=1, \dots, n} d(c_a, c_{b_i})\right) = D\left(\min_{i=1, \dots, n} \sum_{j=1}^t (c_{a_j} - c_{b_{ij}})^2\right)$$

After calculating b' via the above formula, the inquirer obtains the best matching target. During the entire matching process, the proxy computing node and the inquirer cannot access other user's data before encryption, and the privacy of the user data is ensured.

Smart Contract

A smart contract is a digital version of a traditional contract. Once written, it can be trusted by all parties, without requiring trust between those parties. The terms of the contract are final and therefore cannot be changed. This idea was proposed back in 1994 by cryptographer Nick Szabo, but the full potential was not widely recognized until the emergence of blockchain technology. Essentially, a smart contract is a computer program running on a blockchain database that can be triggered by preprogrammed conditions. Blockchain technology brings a decentralized, unchangeable and highly reliable system for an extensive range of applications. Smart contracts are one of the most important features of the blockchain and a key factor in its reputation as disruptive technology that is revolutionizing our social structure.

Lemo's smart contract supports Java, C/C++, Python and a range of other coding languages. All smart contract source code is compiled into bytecode to run in the virtual machine.

The use of Sandbox technology has been implemented to achieve a complete isolation of affairs and limit access to computing resources, whilst maximizing performance and security.

Lemo's smart contract virtual machine is built on a LLVM (Low Level Virtual Machine)-based compiler architecture. LLVM supports JIT (Just-In-Time Compilation) technology, which can dynamically compile and execute the generated machine code according to the users' requirements, which can significantly increase the execution speed of dynamic languages and maximize the performance of hardware. Based on LLVM's powerful three-stage design, future Lemo smart contracts will also support JavaScript and other more languages, and developers who are most comfortable with different technical backgrounds will develop smart contracts. Smart contracts include

the four parts of contract registration, triggering, execution and cancellation:

Contract Registration

Contract registration is the process of storing the consensus in the blockchain after processing the user-written contract security check. Users need to consume gas according to the amount of code required to register a contract.

Contract Triggering

Contract triggering is the process of triggering contract execution through external conditions after contract registration. It supports timing triggering, event triggering, transaction triggering, and other contract triggering methods. Timing trigger refers to the process of automatically triggering the contract call after the node triggers the time consensus after meeting the preset time in the contract. Events, transactions, and other contract calls are new requests that trigger contract execution during the consensus process.

Contract Execution

Contract execution is the complete process of running the contract code in an external environment, including the contract structure mirroring environment, code execution, the implementation of state changes in the implementation of the code and exception handling of the consensus. There is a special message call named a proxy call. Except for the code of the target address being executed in the caller's context, everything else is the same as the message call. This means that the contract can dynamically load code for other addresses at runtime. Only the code is obtained from the caller, this allows us to easily package code into libraries and reuse them in other contracts. For example, to implement a complex data structure, reusable code can be applied to contract storage

Contract Cancellation

Cancellation is only necessary to clean up a contract that has been executed, expired or faces changes in business requirements that are no longer needed. The cleanup process requires a multi-node consensus before it can be completed. The only way to

remove code from the blockchain is to have the Lemo contract perform a self-destruct operation on its address. The remaining balance under this account will be sent to the specified target, and the storage and code will be removed from the stack.

Lemo provides some of the standard contract implementations. Including the consistency check of assets, automatic integration, multi-signature, automatic settlement and other relatively simple logic of the contract. Users can invoke or adapt these contracts to suit their own business needs. It can also be completely implemented by itself.LemoChain

Application Layer Services

Lemo provides some of the standard contract implementations. Including the consistency check of assets, automatic integration, multi-signature, automatic settlement and other relatively simple logic of the contract. Users can invoke or adapt these contracts to suit their own business needs. It can also be completely implemented by itself.

Account System

In a decentralized blockchain world, the user's possessions can only be mastered by themselves, no one person nor organization can steal money, and there is no possibility of it being stolen by server hackers. But in fact, most users can not properly manage their accounts private key. According to Deloitte, at least 37% of users forget the password when they log in and use the "retrieve password" feature. Forgetting the private key on the blockchain will cause the property to disappear directly, and there is no way to get this property back. The total amount of bitcoin having disappeared has reached 4 million, accounting for nearly 20% of the total amount. Users have a very strong demand for secure hosting of private keys.

LemoChain's account system addresses the mapping of user identities to blockchain addresses, user privacy confidentiality, and regulatory audit traceability issues. It allows users to use easy-to-remember usernames and passwords for access and implements OAuth2.0 authentication mechanisms. Third-party applications that obtain user authorization can easily obtain basic Lemo White Paper 28 user information without the management logic of implementing and maintaining user-accounts by themselves. This boils down to just a few lines of code in accessing the LemoChain ecosystem.

Based on the account system, LemoChain will provide some common business unit plug-ins, which can be rapidly integrated into developers DApp applications. This

greatly shortens the project development cycle.

- Online Safe. Encrypting the private key and hosting the backup online. Can only be retrieved by the user.
- Contacts. Manages and maintains many token addresses held by users, as well as address information of recent transactions.
- Points system. Supports multiple dimensions and digitizes user behavior. Accumulation and summation serve as a measure of the user's loyalty and contribution to the platform and can be used as an operation method to motivate users.
- Credit system. Through some basic real-name authentication services, the user's initial credit is evaluated, and the assessment results are continuously revised according to the user's late performance. The entire assessment result will be written as a credit record in the blockchain, providing a strong credit basis for buyers and sellers of data transaction software.
- Authority Configuration. Allows the establishment of authorization relationships between accounts and accounts, accounts and applications. Create higher-level data flow control logic through permissions and licensing mechanisms.

Online Safe

The online safe is a secure private key hosting service provided by Lemo. It is designed to ease the security burden on users. First, the local client encrypts the user's private key and uploads it to Lemo's private key coffer. When the user's private key is lost, the encrypted private key can be retrieved by providing authentication information and decrypted locally. The private and password in the entire process will not appear on the Internet, nor will it appear in the Lemo server. Private key security is guaranteed. Only users themselves can decrypt private data stored on the network.

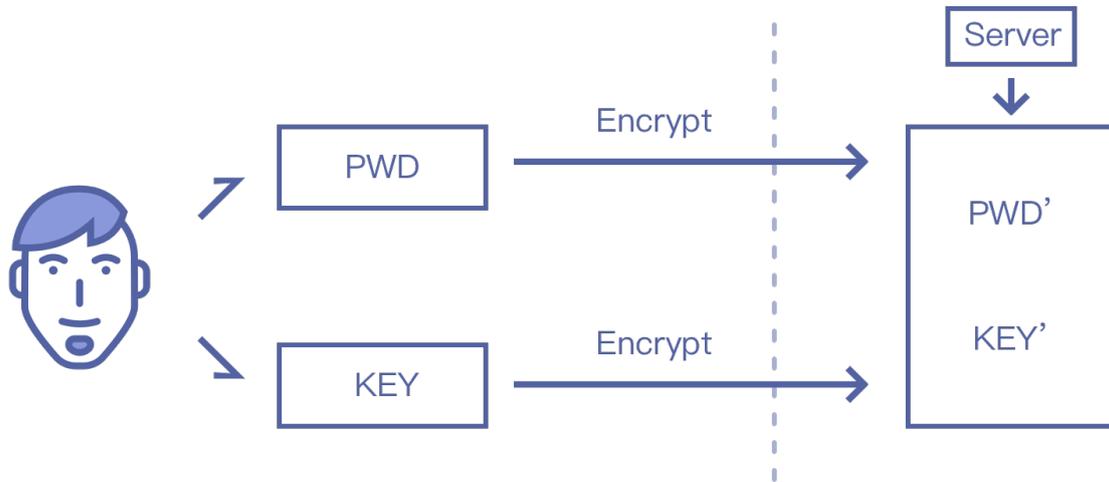


Figure 1 Hosted Private Key

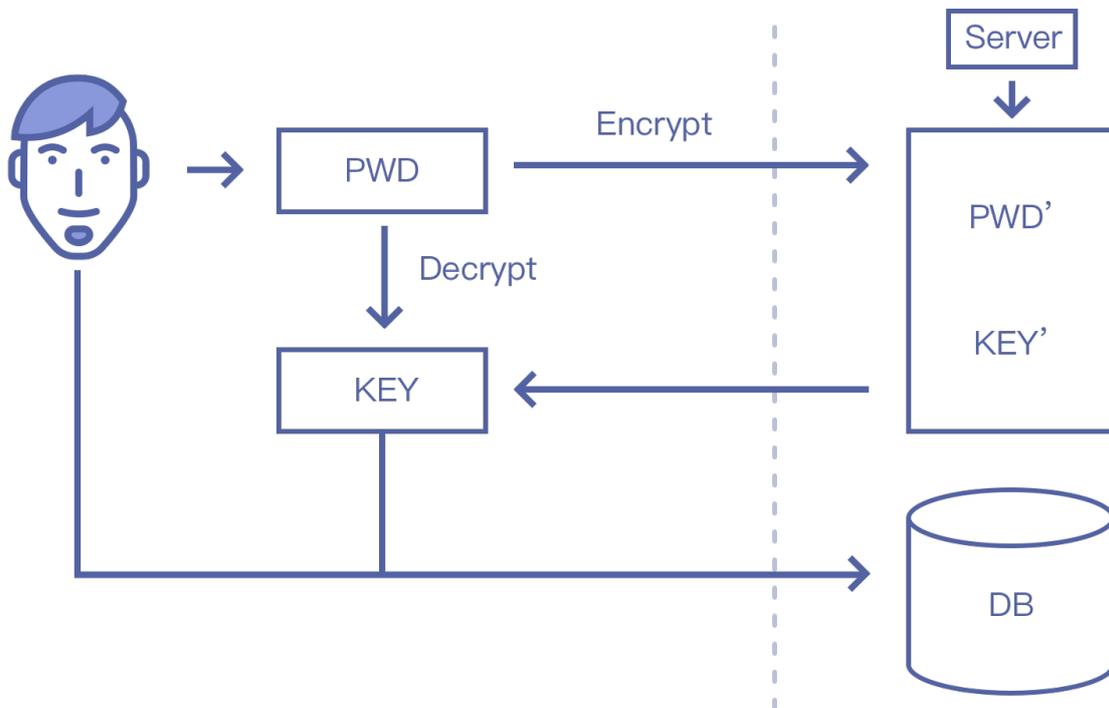


Figure 2 Retrieve the private key

To avoid possible malicious attacks causing data leakage from the server database. The key storage of the online safe deposit box will adopt three-party encryption technology, and the data will be encrypted and stored by an isolated third-party server. Even if the encrypted private key data is stolen, any available real information cannot be restored.

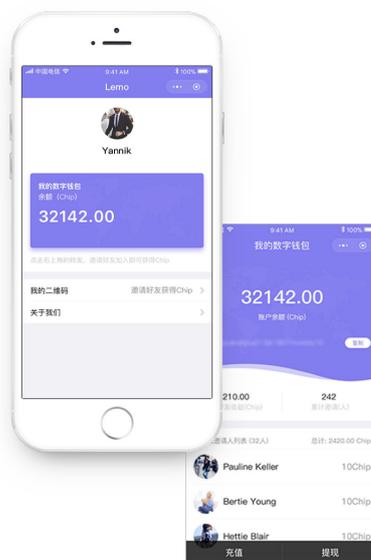
Data Exchange Template

In order to help developers realize the potential of data transaction functions of their respective industries faster, LemoChain has implemented a set of decentralized data transaction system applications based on the team's past experience in social networking and online dating. All the matching requirements are placed on the chain as transaction data, and the smart contract is used to automatically match the transaction. When the match is successful, both parties send data to decrypt each other's private key, ensuring that the user's privacy can be seen only if both parties match. The entire transaction process is open and transparent, privacy information will not be leaked to third parties, and exchanges cannot be concealed from fraud. This application shows developers the smart contract of LemoChain and the use of various services; It is the best developer learning material and can be used as a template to derive data transaction applications in other fields.

Lemo Wallet

We have developed a wallet application for Lemo in order to facilitate Lemo token holders checking their balance, inquiring and tracing transactions and reward records, also receiving related news about LemoChain community. Currently, it only applies to iOS (being reviewed) and Mini-Program on WeChat.

iOS App LemoChip



Mini Program LEMO

Application Prospects Based on LemoChain

LemoChain is developed on a decentralized blockchain network with a platform capable of supporting tens of millions of active users daily. Through adopting a standardized and decentralized storage mechanism, LemoChain will reduce participation costs for all concerned parties.

LemoChain's ecosystem architecture is as follows:

- For Developers: We open Data Exchange APIs, Statistical Analysis APIs and Deep Learning APIs
- For Businesses: Data Trading, Algorithmic Trading, DAPP Enterprise
- For the Open Source community: Availability of results from LemoChain's blockchain R&D

Multiple industry support

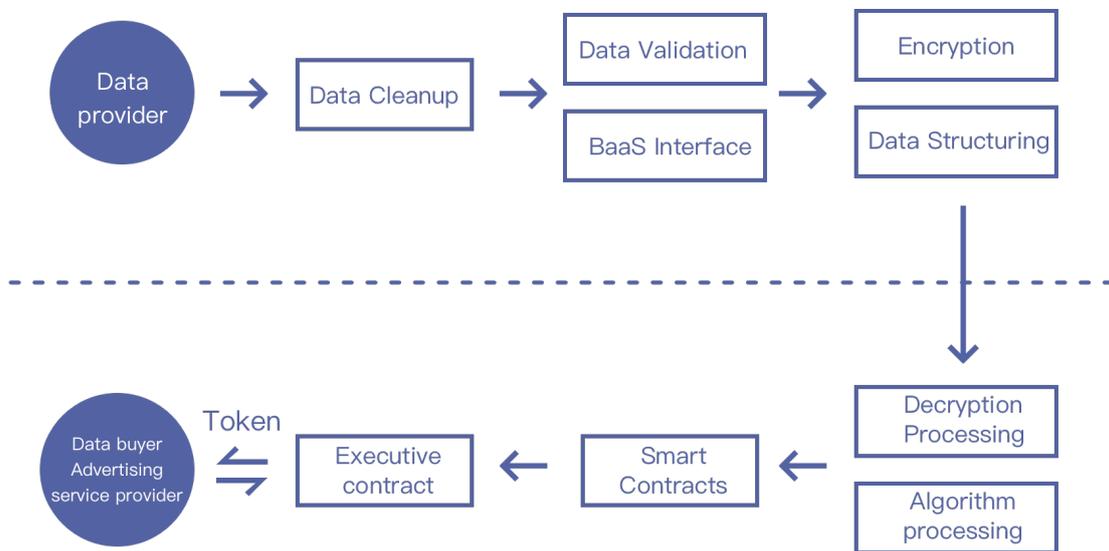
Within LemoChain's ecosystem, there will be regular adaption and introduction of consensus mechanism developments to adhere to ever-changing industry requirements. LemoChain will support multiple industries which have flaws in credit and data exchange, whilst providing the corresponding technical support to ensure businesses remain consistently in-tune with blockchain. Some industries include: social media, education, recruitment etc. Furthermore, based on the data circulation, smart contracts and credit system of LemoChain, we can utilize more complex business logic support through the Turing complete programming language.

Application scenario

Lemo started socializing. As early as 2016, the Lemo team tried to exchange data between several social products of its own to increase the reuse rate of excess traffic, which greatly increased the earnings of various APPs. At the time, our overall payout ratio increased from 6.5% to 11.5%. In a matter of months, turnover nearly doubled.

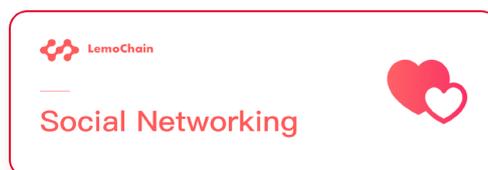
Only the data sharing between several APPs can achieve this effect. Assuming that more merchants can join, the benefits for merchants can be imagined.

But when we try to invite more social APPs to participate in it, the trust issue becomes the biggest obstacle. This made us aware of the current strong demand for data sharing and the enormous difficulties faced by businesses. The characteristics of blockchain decentralized storage and data rights–enforcement technologies, as well as the underlying economic value system, perfectly solve this problem. Lemo was born to solve these problems.



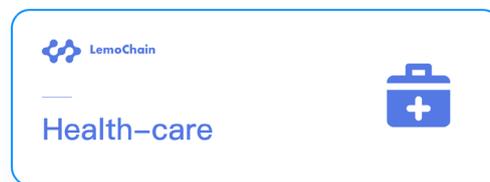
Application Scenario One: Dating

Users submit their personal data and their friends’ needs through dating and dating DApps. Individuals can encrypt and store their social data, and then digital assets can be uploaded to the profitable platform and the tokens can be obtained. Advertisers and their other dating partners need to pay tokens to obtain this data. They can be used for precise matching of dating friends and precise targeting of advertisements.



Application Scenario Two: Health and Medical Data DAPP

Through health data DAPP, personal health data can be securely protected, data can be shared, and users can easily use it. Individuals upload their own health data to profitable data platforms and can obtain tokens. Data providers such as medical service providers and pharmaceutical companies can directly obtain data from profitable data links, and there are huge application scenarios in the direction of new drug development, testing, and precision medical care.



Application Scenario Three: Blockchain technology applied to education and human resources

In the education and training industry, there will be various language training institutions and quality education and training institutions. These institutions are not actually competing with each other, and they can share resources and communicate with each other. However, the current situation is that these organizations have each spent a lot of manpower, financial resources, and time costs, access to market resources (of which there are always some resources are ineffective resources). If Lemo solves the problem of inter-agency trust and student ownership, it can share resources in the form of co-enrollment, increase the number of students, reduce the cost of obtaining customers, and increase profits, while creating an information platform based on blockchain technology for education, skills, and professional experience. The non-defective modification and time stamping functions based on blockchain technology provide employers with a certifiable source of academic, technical, and professional experience information. This saves the company considerable human and financial resources for background research during the recruitment process. This technical system can also be widely used in the certification of notary, finance, banking and

other industries, and has a wide range of application prospects.



Blockchain technology fundamentally solves the trust problem of data circulation, and then realizes decentralization on the basis of it. LemoChain Ecology will fully support decentralized applications from the technical level, develop different modules such as account systems, credit systems, and data distribution protocols, and provide development platforms and interfaces for different developers and service providers, saving development costs, which helps them to iterate quickly and increase profitability. In addition, incentive strategies to attract more developers to join LemoChain, DApp idea of product, so that ordinary Internet users enjoy the value of blockchain technology.

Lemo ReleaseLemo Release

Creation of Tokens

LemoChain has created its own founding currency, Lemo, which during the pre-sale will be issued as an ERC-20 token and can be converted 1: 1 into a LemoChain based token at the end of pre-sale.

Lemo is about to be published to the LemoChain community members and investors. With a shared vision, they will be working with LemoChain to create value and change the future of data circulation. These members will be the mainstay of community discussion, offering invaluable feedback to LemoChain and even becoming visionaries for its community outreach and future development.

LemoChain created Lemo Token based on Ethereum. Lemo is the digital currency based on the smart contracts and published on the decentralized Ethereum blockchain. The total published amount is 1.6 billion before “mining”, and will annually publish no more than 25 million. The new Lemo based on the main chain of LemoChain adopts a D-PoVP mining mechanism, on the backbone of LemoChain, with contributions to data, storage space and power, community contributions and more.

Lemo's Pre-sale Plan

LemoChain will issue a total of 1.6 billion Lemo before the mine, and 25% (400 million) Lemo tokens will be exchanged for 9,000 Lemo per ETH. It will be allocated to participants in the pre-sale period in two phases: private placement and public offering. A total of 20,000 hard-top ETHs and 2,000 soft-top ETHs are recruited. The pre-sale will be released to different participants in phases from March 2018, and will provide no more than 20% of the credits in the private placement stage according to the participants' contributions. The pre-sale will continue until mid-to-late May 2018, or it will stop within 24 hours after touching the hardtop ceiling.

After the pre-sale period is over, subsequent investors will also be able to obtain Lemo tokens through compliance with all major cryptocurrency transactions. Lemo will gradually start the global cryptocurrency exchange in early June.

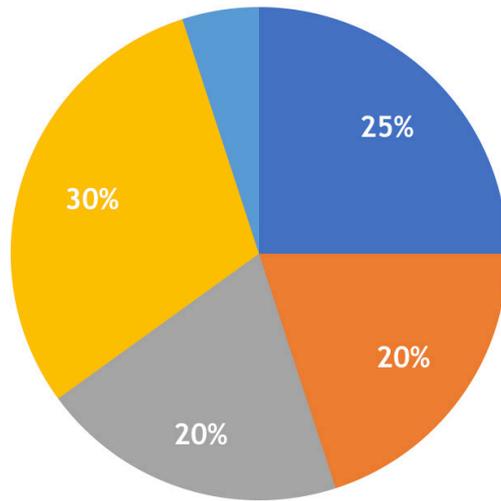
The Lemo Token is a vehicle for the transmission of data values. It has the property of quantifying the value of data within the Lemo Ecosystem, but it does not participate in the circulation outside the Lemo Ecosystem in any way.

Overview

Lemo Token Pre-sale Overview

Description	Volume
Pre-mining	1,600,000,000 Lemo (100%)
For Pre-sale	400,000,000 Lemo (25%)

- 25% of Lemo before mining will be created and distributed to the participants at their smart contract addresses at the pre-sale stage. Participants can check it via the wallet application of LemoChain or Ethereum network;
- 20% of Lemo before mining will be created and distributed to early-stage investors of LemoChain;
- 20% of Lemo before mining will be used for early user stimulation, rewarding users and developers joining in to develop the ecosystem and community of LemoChain;
- 30% of Lemo before mining will be created and distributed to the core developers, founders, teams, and partners of LemoChain. It is bound to a 24-month period smart contract, which executes once every 6 months;
- 5% of Lemo reserve will be locked for at least 12 months as a strategic buffer, and periodically and gradually assigned to new contributors. The premise should be beneficial to the growth of the entire Lemo community. Otherwise, these reserves will be withdrawn and reallocated.



■ Pre-sale ■ Early Investors ■ Community Stimulation ■ Core Team ■ Reserve

Budget

Funds raised during the pre-sale period will only be used to help LemoChain's ecosystem development and expansion. LemoChain's technical research shows the viability of these technologies in related fields, but also recognizes that the work of the Lemo community has a long way to go.

Below is a budget plan:

40% Core development

Core development includes the core techniques of LemoChain as well as the development of smart contracts and the decentralized ecosystem. A majority of this budget will be used for building basic framework, improving user experience and developing new functions.

20% Security

The undergoing foundation relies on the security of LemoChain's blockchain. We are planning a series of security inspections, and each new function must be inspected thoroughly before going online to the main network.

25% Marketing

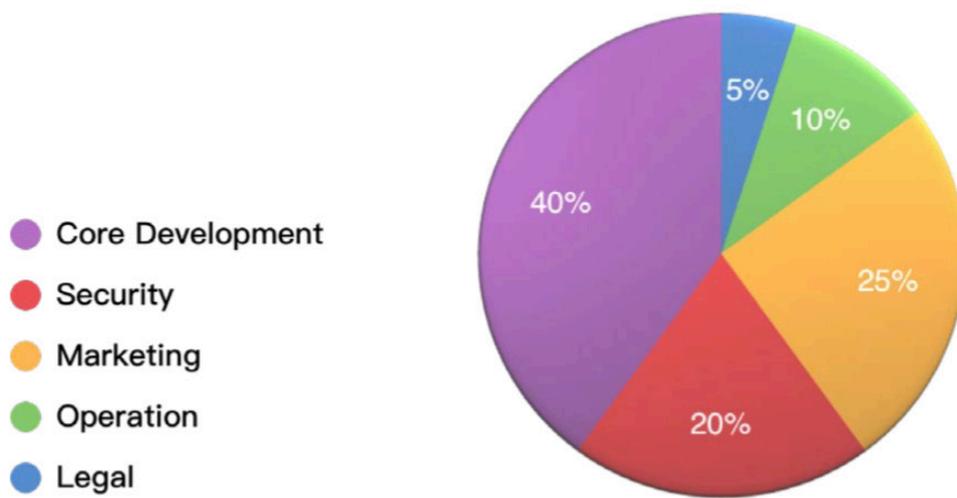
Given the reward mechanism of the previous Lemo platform, we will reward and support early contributions of quality developers and encourage users to invite more potential community members in order to remain continually prosperous.

10% Operations

To ensure the smooth operation of the whole network, Lemo Foundation will pay more attention to the operation and management of community, and will globally seek resources useful for ecosystem development.

5% Legal

Legitimacy is the key to the long-term success of LemoChain, so we will delegate a portion of the budget to legal expenses, to ensure it is legal under all sorts of inspections when LemoChain goes global.



Unlocking plan of early token holders

To ensure the long-lasting success of the LemoChain community, early token holders of Lemo will meet a lock-up period, details are the following:

Founding Team

Lemo tokens held by the founding team can only be periodically liquidated. Additionally, every withdrawal needs the support of the Foundation’s decision-making committee.

	Time	Proportion
First time	2018.10	12.5%
Second time	2019.04	12.5%
Third time	2019.10	12.5%
Fourth time	2020.04	12.5%
Fifth time	2020.10	12.5%
Sixth time	2021.04	12.5%
Seventh time	2021.10	12.5%
Eighth time	2022.04	12.5%

Early Investors

After pre-sale stage, Lemo held by early investors will be deployed in four phases. On the day of being listed on the first exchange, 25% of Lemo will be deployed, the following 25% will 30 days later, and the final 50% will be deployed in 25% installments for every 45 days.



LemoChain's Governance Ecological Framework

In order to realize LemoChain's sustainable development and avoid the development of loose sand-type development structure and underlying structure, Lemo Foundation LTD (Lemo Foundation), a non-profit organization registered in Singapore, will be responsible for overseeing the fairness and productivity of the ecosystem. Growth, meanwhile, will establish a sound governance structure, establish a standing committee, and manage issues such as code management, financial management, compensation management, iterative update management, and privileged operations. At the same time, the Standing Committee continued to update the development of foundations and communities, and introduced supervision and supervision mechanisms, rulemaking and change control management. In the end, the Lemo Foundation will promote the transition of the entire ecosystem to a fully decentralized and autonomous network. Lemo Foundation LTD will fully cooperate with partners to integrate resources such as government, enterprises, technology, business, and universities, maximize resources sharing, use resources efficiently, and realize social collaborative development.

At the same time, Lemo Foundation LTD will also provide transparent financial management, comprehensive code management, technology research and development, marketing, security research and development management, and help LemoChain commercial promotion. At the same time, the Foundation will actively promote high standards of ethical and honest business practices and comply with relevant laws and regulations. In addition, Lemo Foundation LTD will employ third-party authorities to pass audit reports of related work, compliance supervision and supervision of LemoChain's development. Lemo Foundation LTD.

Lemo Foundation LTD

The Lemo Foundation LTD (hereafter referred to as the "Lemo Foundation") will be dedicated to promoting LemoChain's R&D, governance, and promotion efforts, and will drive the security and harmonious development of the entire LemoChain open source ecosystem. It will be open, fair and transparent and not profitable. Operate LemoChain. Lemo Foundation LTD is a Non-Profit Entity that will be approved by the Singapore Accounting and Enterprise Regulatory Authority (ACRA) and is regulated by Singapore company law. The foundation is independently managed and operated by a board of trustees or a management committee (ie, the decision-making committee below) that includes natural or legal persons entrusted with the foundation. According to Singapore law, the Lemo Foundation is a legally formed organization that does not have any commercial interest to support or participate in public or private interest activities. Its "profit" is called surplus and will continue to be reserved for other activities without being distributed among its participants.

The Lemo Foundation will establish content review and operations committees that comply with local regulations in the course of activities in different countries to ensure its worldwide compliance.

The multiple forks of Bitcoin and Ethereum have led to questions about the decentralization of Ethereum or blockchain. To avoid diverging situations, the Lemo Foundation will develop a good governance structure to help and promote the harmonious development of the entire community.

The Lemo Foundation was established to ensure the sustainability of the entire community and its open source projects, the safety of raised funds, and the management of its communities. The initial stage of the Foundation will consist of a founding team consisting of a decision-making committee, an R&D code review committee, a property and personnel committee and a market public relations committee. The decision-making committee consists of the first chairman of the Foundation Andrew, LemoChain core R&D personnel and early investors, each for a period of two years.

Future decision-making committee seats will also be opened to more participants after the increase in the number of organizational structures and participants.



LemoChain Founding Team

The LemoChain team is made up of high-tech people from Silicon Valley, Singapore, London, and China. It combines technological innovations in Silicon Valley, high-efficiency in Singapore, financial data capabilities in London, Tencent, and high-quality research and development of companies such as 360. The team has years of experience in building and processing massive user data and is dedicated to using blockchain technology to enhance real life and business efficiency. The "mobile-oriented" strategy will promote the productization of blockchain technology and increase the industry ease of use of blockchain technology, and use blockchain to build a bridge for real-world business social data exchange:

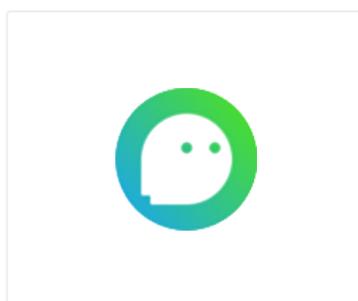
Current team core member

Please refer to the official website of the latest information: www.lemochain.com

Lemo Advisory Team

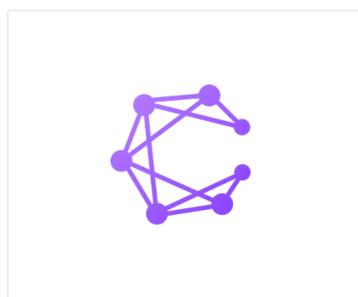
Please refer to the official website of the latest information: www.lemochain.com

Lemo's strategic partners



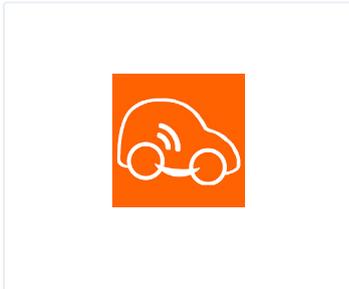
LemoChain collaborates with Xiao Jingling, the mainstream education management platform in China. Based on LemoChain development, the blockchain module will cover tens of millions of users after it goes online

In August 2018, XiaoJingling, an online educational application based on LemoChain, will be launched to enhance secure and accessible educational resource distribution services for hundreds of educational institutions and nearly one million parents in China. The number of users is set to increase to around 10 million by the end of 2018.



LemoChain and Chengdu Metropolitan Technology Co., Ltd. reach strategic co-operation

July 2018, business social APP Lemon VCard will be published based on the LemoChain, using blockchain technology to solve business transactional trust issues. It will provide a secure digital business identity for companies operating on Lemo. Lemon VCard is currently available on the WeChat mini-program. IOS version is expected for August launch and will be available world wide.



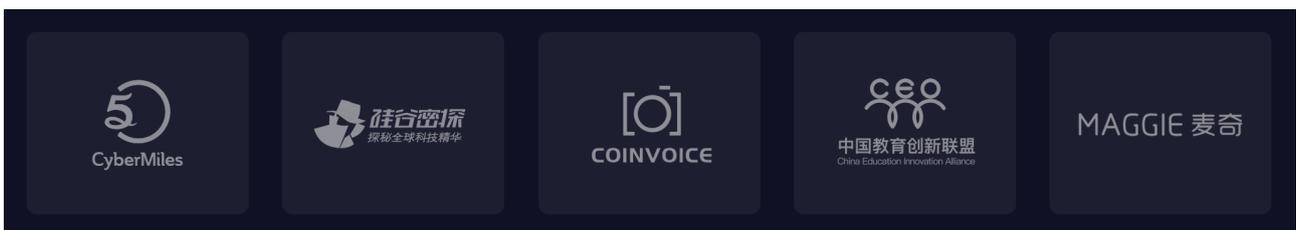
LemoChain and China Panda Driver Open a New Chapter of Smart Contract Transport Services,available to Panda Driver’s 8 million current users

LemoChain and China Panda Driver Open a New Chapter of Smart Contract Transport Services,available to Panda Driver’s 8 million current users.



LemoChain and US social networking company Inspiration Tech LLC form strategic partnership to create a DApp that would be accessible by 6 million users

In June 2018, Inspiration Tech will complete and improve it’s dating product Kuku based on LemoChain, using blockchain technology to solve practical problems such as scammers and fake profiles.

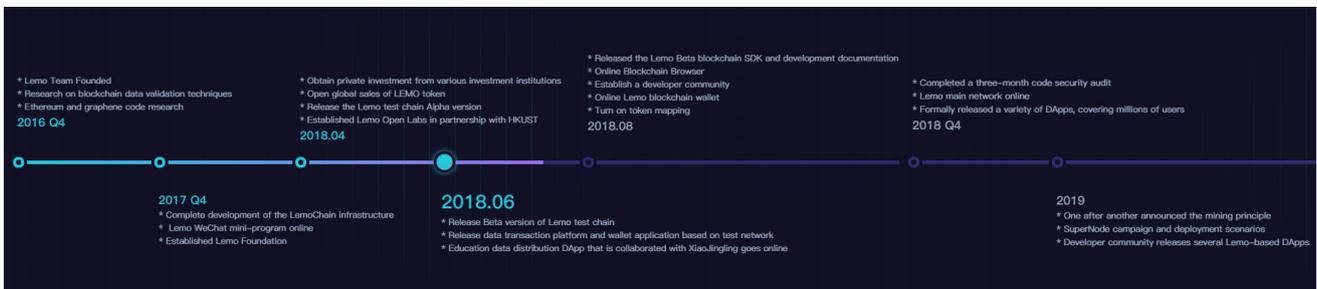


Due to the confidentiality terms, more information on consultants, strategic partners and investors will be provided after signing the confidentiality agreement.

Contact email: foundation@lemochain.com

Lemo's execution and iteration

Timeline



Lemo Pre-sale plan

LemoChain's users and their developers acquire LemoChain's capabilities by consuming Lemo, especially when LemoChain runs distributed applications that pay for and consume a certain amount of Lemo tokens. All digital asset transactions in the LemoChain network will be settled in Lemo tokens.

LemoChain pre-mine tokens will be produced at the time of the release of LemoChain and will be held by the LemoChain Foundation. ERC-20 Lemo tokens held by early holders can be exchanged 1:1 at this time.

Lemo's public pre-sales of the specific rules and information will be announced through the LemoChain official website and Lemo wallet application and public number, please pay attention.

Participating in the Lemo Foundation's pre-sale of Lemo tokens is not risk-free. For detailed risk content, please refer to Lemo's exemption and risk description.

Lemo iterative planning

As an early application of emerging technologies, blockchain technology faces various challenges and opportunities. LemoChain's Future Iteration Directions:

- One is the iteration of the underlying architecture code;
- The second is the iteration of commercial applications built on the main chain of LemoChain.

The iteration of the LemoChain infrastructure

When the LemoChain architecture code itself is flawed, it is usually iterated through the system upgrade. Vulnerabilities need to be analyzed, tested and reviewed by the Code Review Committee and submitted to the Decision Committee for reporting. The following are definitions of major vulnerabilities:

- Affect user's asset safety
- Major security incidents
- System security issues
- System operation logic does not match the design

When the Lemo Ecology cannot meet the needs of business and users of the participants, it is usually adopted by opinion leaders to represent the interests of the community. After the decision-making committee has passed the decision, the developers of the organization are responsible for the development. The development committee completes the analysis of the code committee, tests and reviews, and reports Prepare the way for the decision committee to iterate.

Business application iteration

Lemo is a global open source project that connects blockchains to the real world

through technological innovations and conceptual innovations. With regard to the iteration of commercial applications, the Foundation will select the appropriate third parties to cooperate in the industry and application iterations, led by third-party developers, and provide technical support to Lemo.

Lemo's Disclaimer and Risk Statement

Disclaimer

Except as explicitly stated in this white paper, Lemo Foundation LTD and its cooperating agencies will not make any representations or warranties (especially for its merchantability and specific features) to LemoChain or LEMO tokens.

The pre-sale plan for people to participate in the purchase of LEMO tokens is based on individual's own desire to learn about LemoChain and LEMO Tokens.

Without prejudice to the generality of the foregoing, all participants will participate in the LemoChain project after starting to accept Lemo tokens as they are, regardless of their technical specifications, parameters, performance or functions.

LemoChain hereby expressly disclaims and refuses to assume the following responsibilities:

- Any person who violates any country's anti-money laundering, anti-terrorism financing, or other regulations when purchasing LEMO tokens;
- Any person who participates in the pre-sale of LEMO tokens and violates any statements, warranties, obligations, commitments contained in this white paper;
- Promises or other requirements, and the resulting inability to pay or receive Lemo tokens;
- Pre-sale plans for LEMO tokens are abandoned for any reason;
- Failure or delay in the development of LemoChain and the resulting failure to

deliver LEMO tokens;

- Concerns caused by technical issues such as bugs, errors, defects, crashes, rollbacks, or hard forks of the relevant blockchain source code;
- Use of funds raised from presales;
- Any participant who has disclosed, lost or damaged their wallet private key for their digital wallet;
- Defaults, violations, infringements, collapses, defects, termination or suspension of services on third-party platforms involved in the pre-sale of LEMO Tokens;
- Fraud, misuse, misconduct, error, negligence, bankruptcy, liquidation, dissolution or closure;
- Anyone's transaction or speculation on LEMO tokens;
- Listing or delisting of LEMO tokens on any exchange;
- LEMO tokens being classified or regarded as a currency, securities, commercial paper, by any government, competent authority, or public agency.

Risk statement

The LemoChain development and operations team believes that there is nothing in the development, maintenance and operation of LemoChain.

There are a number of risks, many of which exceed the control of LemoChain's current development and operations team which need to be considered by participants, except for those described in this white paper

In addition to other content, each pre-sale participant of LEMO tokens should also peruse, understand, and carefully consider the following risks before making investment decisions.

Purchasers of LEMO tokens should pay special attention to the fact that despite the management master developed and operated by LemoChain, which was established in Singapore; both LemoChain and Lemo tokens exist tangibly only in cyberspace and

are not registered to a single country. Participating in this pre-sale should be a well-thought-out decision-making action that will be considered as participants fully aware of and agreeing to accept.

The following risks:

1) Termination of Presale Plan

The LEMO token Pre-sale Plan may be terminated prematurely, at which point the participant may be subject to the fluctuations in price of Bitcoin/Ethereum. As a consequence of the fluctuations in the market and the expenses of LemoChain's development and operations team, investment amounts may only be partly refunded.

2) Insufficient information provision

As of the publication date of this white paper, LemoChain is still in the development phase. Its philosophy, consensus mechanism, algorithm, generation codes as well as other technical details and parameters may be updated and changed frequently. Although this white paper contains LemoChain's latest key information, it is not absolutely complete, and will still be used by LemoChain's development and operations team for specific purposes to make adjustments from time to time.

LemoChain's development and operations team is incapable of, and has no obligation to inform participants at any time; every necessary detail of LemoChain's development (including its progress and expected milestones, whether or not postponed) will be published, so there is no need for communication.

However, the pre-sale participants will promptly and fully reach out to the information released by LemoChain from time to time. Information disclosure is not fully unavoidable and reasonable.

3) Regulatory Measure

Encrypted tokens are being or may be supervised by the authorities of various countries.

Any risk factors disclosed in this white paper, as well as those associated with such risk factors, resulting or consequential damage, loss, claims, liability, penalties, costs, or other negative effects.

The team may from time to time receive enquiries, notices, warnings, orders or rulings from one or more authorities, or even may be ordered to suspend or terminate any action regarding this pre-sale plan, LemoChain development or LEMO tokens.

LemoChain's development, marketing, promotion or other aspects as well as this pre-sale program may be seriously affected blocked or terminated. Since the regulatory policy may change at any time, the existing LemoChain project or the regulatory approval/tolerance of pre-sale plans may only be temporary.

LEMO tokens may be defined differently at any time in different countries as virtual goods, digital assets and even securities or currencies, so in some countries, according to local regulatory requirements, LEMO may be prohibited from trading or holding.

4) Cryptography

Cryptography is constantly evolving and it cannot guarantee absolute security at all times. Advances in cryptography (eg password cracking) or technological advances (such as the invention of quantum computers) may present threats to cryptography-based systems (including LemoChain) This may result in the theft, disappearance, destruction, or devaluation of any held LEMO token.

In a reasonable range, internally, the LemoChain development and operations team will prepare itself to take preventive or remedial measures to upgrade the foundations of LemoChain.

Agreeing to respond to any advances in cryptography and, where appropriate, incorporate new and reasonable security measures for cryptography and security.

5) Development Failure or Abandonment

LemoChain is still in the development phase, and does not have the ready-to-release finished product. With the technical complexity of an ecosystem like LemoChain, the

development and operations team may face unpredictable and/or insurmountable difficulties from time to time. Therefore, the development of LemoChain may fail or be abandoned at any time for any reason (e.g. due to lack of funding or development failure) This will result in Lemo tokens not being delivered to any participants in this pre-sale program.

6) Theft of Crowdfunding Funds

There may be attempts to steal the pre-sale cryptocurrency tokens received by the LemoChain platform. Theft or stealing attempts may affect LemoChain's development and operations team's ability to fund the development of the project. Despite LemoChain's development and operations team adopting cutting-edge technology solutions to protect the security of pre-sale funds, hacking and theft of funds is never fully preventable.

7) Source Code

No one can guarantee that LemoChain's source code is completely flawless. Code may have certain flaws, errors, bugs, and vulnerabilities that may make it impossible for users to use specific features, expose user information, or create other problems. If this is the case, it will impair the usability, stability and/or security of LemoChain and therefore have a negative impact on the value of LEMO tokens.

8) Security Weaknesses

The LemoChain block chain code is open sourced. Although the LemoChain development and operations team works hard to maintain system security, anyone may intentionally or unintentionally bring vulnerabilities or defects into LemoChain's core infrastructure elements, which LemoChain's development and operations teams cannot implement sufficient security measures to prevent or make up. This may eventually result in the loss of participants' Lemo tokens or other digital tokens.

9) Distributed Denial of Service Attack

Ethereum publishing their founding tokens was designed as an open and unlicensed account. Therefore, Ethereum may suffer from time to time from "Distributed Denial

of Service” cyber attacks, which will negatively impact, stagnate, or paralyze the Lemo token system.

As a result, transactions on top of this are delayed or written into blocks in the Ethereum blockchain, or are even temporarily unavailable.

10) Insufficient Processing Capacity

The rapid development of LemoChain will be accompanied by a sharp increase in trading volume and subsequent increased demand for processing capacity. If the processing capacity demand exceeds the load that can be provided by the nodes within the blockchain network, the LemoChain network may falsify or stagnate. Resultantly, fraudulent or erroneous transactions such as ”double spending” may occur. In the worst cases, anyone holding LEMO Tokens may lose them potentially triggering an Ethereum network rollback or even a hard fork. The aftermath of these events will damage the usability, stability and security of LemoChain and the value of LEMO tokens.

11) Unauthorized Claim for Sale of Lemo Tokens

Any person who obtains the token holder’s registered email or account access rights by decrypting or cracking the LEMO token holder’s password will be able to maliciously obtain pre-acquisition from LEMO token holders. Accordingly, LEMO tokens obtained by the holder may be mistakenly sent to anyone who claims LEMO tokens through the holder’s registered email or registered account, and such sending is irrevocable and irreversible. Each Lemo token pre-sale participant shall take measures such as those below to properly maintain the security of his/her registered email or registered account:

- (i) Use high security passwords;
- (ii) Does not open or reply to any fraudulent emails;
- (iii) Strict confidentiality of or personal information.

12) Lemo Token Wallet Private Key

Loss or corruption of private keys necessary to obtain LEMO tokens is irreversible. LEMO tokens can only be manipulated using a local or online LEMO token wallet with

a unique public and private key. Each pre-sale participant should properly protect his/her LEMO token wallet private key. If the LEMO token holder's private key is lost, lost, leaked, damaged or stolen, neither the LemoChain development and operations team nor any other person can help the holder to obtain or retrieve the relevant LEMO tokens.

13) Popularity

The value of Lemo tokens largely depends on the popularity of the LemoChain platform. LemoChain does not expect immense popularity, or common use within a very short period of time after the release. In the worst case, LemoChain even may be marginalized for a long period of time, attracting only a small group of users.

In contrast, a large part of LEMO token demand may become speculative in nature. Lack of users may lead to an increase in price fluctuations in the Lemo token market and thus affect LemoChain's flood season development of. When this price fluctuation occurs, the LemoChain development and operations team will not (and take no responsibility for) stabilize or influence the market price of LEMO tokens.

14) Price fluctuations

If you trade in the open market, encrypted tokens usually have sharp price fluctuations. In the short term, price shocks often occur. The price may be quoted in Bitcoin, Ethereum, U.S. Dollars, or other legal currency. This price volatility may be caused by market forces (including speculative trading), changes in regulatory policies, technological innovations, the availability of exchanges, and other objective factors, which also reflect changes in the supply-demand balance. Regardless of whether or not there is a secondary market for LEMO token trading, the LemoChain development and operations team is not responsible for LEMO token transactions in any secondary market. Therefore, the LemoChain development and operations team has no obligation to stabilize the LEMO token's price fluctuations. The risk involved in the transaction price of LEMO tokens must be borne by LEMO token holders.

* 由于保密条款的约束，关于早期投资人的信息将在提出信息请求后，签署保密协议的前提下告知。联系邮箱：foundation@lemochain.com

* 此白皮书仅代表截止 2018 年 4 月 14 日 LemoChain 项目的进展和状态，版本号 2.2 持续更新中

- <https://cryptovest.com/news/cryptokitties-burn-up-15-of-ethereums-gas/>
- <https://bitshares.org/technology/industrial-performance-and-scalability/>
- <https://blockchain.info/charts/n-transactions>
- <https://etherscan.io/chart/bloktime>
- <https://news.bitcoin.com/ethereum-blockchain-congested-cats/>
- GENTRY C. Fully Homomorphic Encryption Using Ideal Lattices[C]//STOC '09. [s.l.]: ACM, 2009: 178