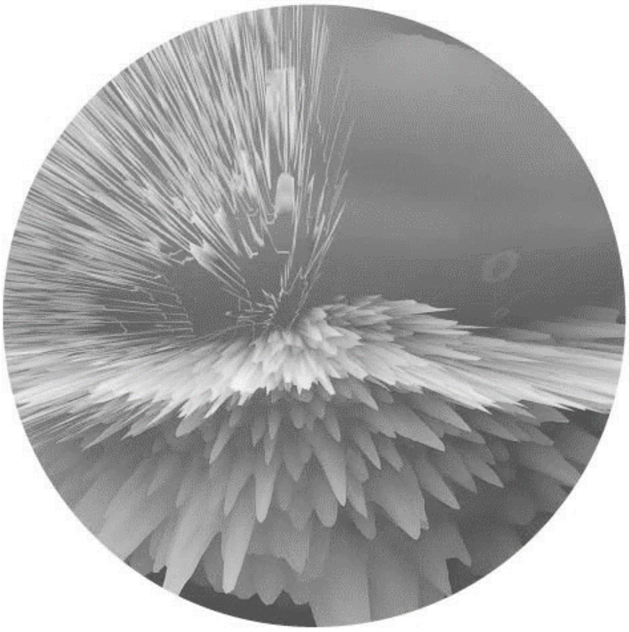
Year
2019

LIBERUM

White Paper

Creating a future-oriented distributed trust ecosystem
in which every person can issue blockchain and realize self-finance



Freedom is a dream
born in the vast sky,
composing the great changes, days and nights,
as well as sun and moon for the true meaning of life.

Freedom is like a lonely island.
When weighing between love and freedom,
she chooses to stay in the island.
After all, the ocean of love is too broad and extensive, without direction.

Freedom is a kind of power,
buried in the deep sea.
It arouses ups and downs for the struggle of life,
with roaring waves and stormy surges.

Freedom is a wing striking violently.
I can uplift the torch of freedom to light up the front.
I can sing happily and fly upward!
We can grow up in a country of freedom.

CONTENTS

1 **Foreword**

2 **Project Introduction**

Project Profile

Project Philosophy

Design Concept

3 **Background of Liberum’s Birth**

Blockchain is the New Generation of Value Internet

Features of the Blockchain Technology

Update and Iteration of Blockchain Network

Common Public Blockchains and Their Characteristics

Prominent Pain Points of Public Blockchain

Liberum arises at the right time

4 **Introduction to the Liberum Project**

What is Liberum?

Vision of Liberum

Mission of Liberum

What Is Liberum’s Subchain

Reasons for Using the Liberum Subchain

Comparison with Other Public Blockchains

CONTENTS

5 Technology Innovation System of Liberum

Public Blockchain of Liberum

Parent Chain: HWD-PoW Innovative Consensus Mechanism

Smart Contract Implemented in the Form of Subchain

Subchain With Customizable Consensus Algorithm

Asynchronous Smart Contract

Blockchain Sharding

Cross-chain Technology Is Ready

Event Processing

Mining

Wallet and Payment System

API

Security

6 Ecosystem of Liberum

Basic Ecology of Liberum

Community

Dividends for DAPP Developers

Decentralized Exchange (in the closed beta test)

Subchain Project

Decentralized anonymous chat software (in beta)

Decentralized anonymous Q&A software (in beta)

CONTENTS

7 Economical Model of Laber

Introduction to Laber

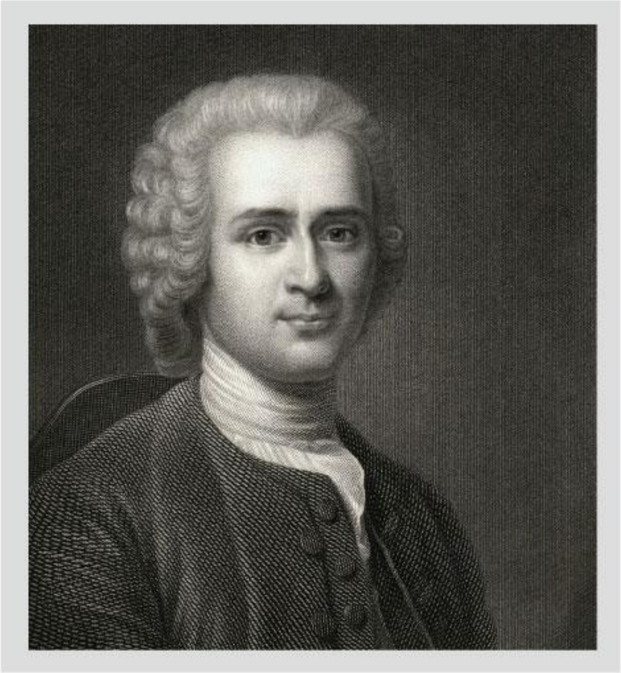
Issuance and Initial Distribution of LBR Public Blockchain

Decentralized Self-governed Community

8 Implementation Route

LIBERUM

Foreword



“ Man is born free and everywhere he is in chains.

——- Jean-Jacques Rousseau

Du Contrat Social ”

Foreword

Man is bornfree and everywhere he is in chains. Freedom is an inherent natural endowment and right of man. However, unfortunately, most of men live in a non-free state, and suffer from slavery to the fullest extent. Internet solves the boundary problem of information circulation, making information and data unblocked, but we have lost the rights to control the data and assets unconsciously. Monopoly allows enterprises to gain profits, but users never enjoy any revenue.

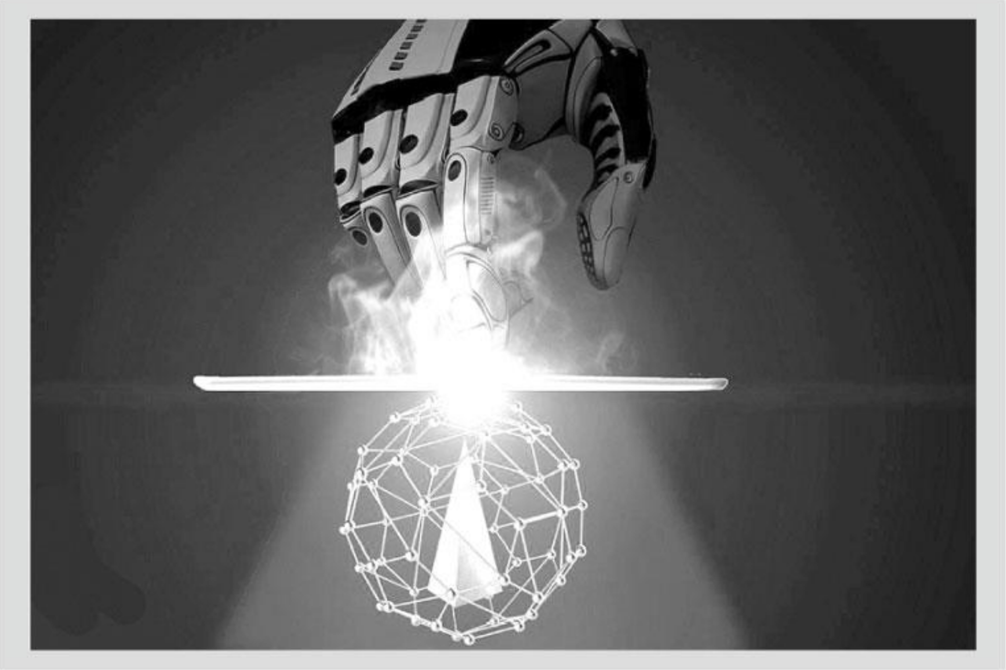
The appearance of blockchain has enabled us to find a way to solve this problem. The consensus system generates passive trust by technological means, and forms a tamper-resistant consensus mechanism, thereby reaching the highest state of trust up to now - dispensing with trust. This is a subversive technological revolution deserving our attention, which has solved the bottleneck of modern human civilization development from the root, so it is worthy of constant exploration and practice by all humans.

However, from the technical perspective, the current mainstream public chain systems have the disadvantages of limited scalability, low processing efficiency, insufficient storage capacity and the vulnerability todouble-spending attacks; from the industrial perspective, it is featured by limited widespread use of technology, long development cycle, greatdifficulty andinsufficient interaction with the real world. Therefore, the blockchain market urgently needs an environment of innovation, democracy, transparency, equality, freedom and security to cope with the upgrading and iteration of the blockchain industry. From the financial perspective, the design philosophy and currency system of Bitcoin have seriously violated the basic attributes, operating laws and value logic of currency, making it difficult to become a universal currency and a payment currency.

We hope that everyone can get the right to freedom and lead a better life. In this White Paper, we propose a solution that comprehensively strengthens all the current distributed ledgers, which we call Liberum.

LIBERUM

Project Introduction



The future has come and everything is possible

“ When we are talking about the future, the future has come; when we are talking about the future possibilities, everything is possible. In the face of the future, we can only embrace the future with an attitude of change and win.

The future seems afar, but the world has changed. The boundaries between the present and the future have become blurred. We have stepped one foot in the present while the other foot in the future. ”

Project Introduction

Project Profile

Liberum strives to develop the third blockchain ecosystem outside Ethereum and EOS. It is a blockchain infrastructure that provides customized services and it is a global blockchain open-source community project. Besides,it implements point-to-point value transfer through a value transfer protocol, and builds a decentralized application development platform that supports multiple industries based on this protocol. Due to innovative technology, perfect governance structure and wide application range, Liberum will become a public chain superior to Ethereum and EOS, thereby reducing the development cost of blockchain and promoting the implementation of blockchain applications.

By introducing off-chain factors, Liberum forms a blockchain master contract that is in line with the real world business logic, supporting multiple industries and multiple channels. In the Liberum ecosystem, we will work with third-party developers to provide mobile services from the technical architecture support, including mobile wallets, mobile DApp applications and mobile smart contract services. Also, we encourage third-party developers to develop the blockchain-based mobile services and jointly promote the implementation of blockchain technology together.

As the most promising blockchain ecosystem, Liberum perfectly combines the advantages of Ethereum, EOS and other public chains, and solves the inherent shortcomings of existing blockchain systems. Liberum will continue to build the basic platform and the development and iteration of various product development and commercialization projects to gradually form a blockchain economy, improve industry efficiency, and promote efficient and coordinated development of society. In addition, Liberum will work with users from all over the world to create a community organization of sharing, shared governance and security.

Project Philosophy

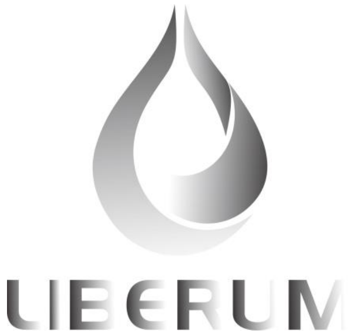
For the global finance, Internet has accelerated the digitization of financial assets. However, during this process, we are restricted by its non-transparency and the limit of Internet itself. At this moment, assets safety and trust crisis have become the greatest threats for personal assets. The appearance of blockchain enables many people to see a hopeful future.

In the current society, people have realized that most social conflicts are caused by centralization. Perhaps, decentralization is the only cure. The blockchain technology has perfectly solved the global trust crisis, and the encryption technology has found a solution for our assets safety. The application of blockchain technology still has a long way to go, and more and more people begin to pay attention to the application value of blockchain, which is just our original intention to design and develop Liberum. It is hoped that our efforts can open a new window for the world and become a significant social practice.

Liberum is not only a single blockchain project, but also an integration of many research results of blockchain-based distributed cloud application. It will play an important role in identity safety, transaction freedom and decentralized finance & commerce. It can be said that Liberumis to rebuild a new open structure in the distributed cloud system, which will lead us to an unprecedented free development space.

The future society will be an entirety linked by blockchain. As a certain product of blockchain technology, Liberum adopts the decentralized design principle, reaching the consensus of wealth, comment, innovation, network and even ideological progress. By connecting the life force, it will completely subvert the traditional digital currency transaction and circulation ecology, promote the progress of human civilization. In this free community, every person is its owner, and the world will get the real freedom.

Design Concept



Liberum Logo is a journey of the soul through the starry sky. It presents the order and rules of the universe, and also connects the subconsciousness of the human being, so that people may concentrate on it and pursue the freedom and eternity of life in the process. Also, it represents an order that creates an infinite future. We believe that digital technology will have a long-term development in the future. In the near future, blockchain assets will become the mainstream of finance.

On the one hand, the Liberum Logo is a symbol of the burning flame, which heralds light, solidarity, friendship, peace and justice, guides people to regain the direction of civilization, and advocates and promotes the spirit of freedom in science and democracy. On the other hand, the Liberum Logo is also a symbol of unstoppable free water droplets, which penetrate through the cloud and crack the stone; there is nothing to fear, even when shattered to pieces.

The Liberum Logo blends water and fire, representing a service platform that pursues fairness, openness and rules, allows the flower of ideas to blossom and to grow, and finally realizes the freedom of wealth and all things!

Here, we will overturn all the existing rules of the traditional social value transmission, reconstruct a new and unprecedented distributed consensus system, and lead global practitioners in all fields into a higher dimensional collaborative form.

Chapter I

Background of Liberum’s Birth

Chapter I. Background of Liberum's Birth

1.1 Blockchain is the New Generation of Value Internet

In the course of human civilization, the society has progressed and changed in the form of survival of the fittest. From the ancient Stone Age to today's era of Internet and the sharing economy, the emergence of each core technologyhas greatly solved the production, economy and communication issues and promoted social progress.

With the rapid development of society and technological progress, unreliable information and lack of credit resources are becoming more and more serious, the trust system between governments, enterprises and individuals has become increasingly fragile, and communication and transaction costs have increased dramatically.

In 2008, Satoshi Nakamoto published a paper titled *Bitcoin: A Peer to Peer Electronic Cash System* in which the concept of blockchain was proposed for the first time, established the technical base for encrypted transmission of transaction information, and structured the Bitcoin network. From then on, digital currency has become the most important application of the blockchain technology, and has gained rapid development.

Since the Bitcoin digital currency platform was established in 2009, the Bitcoin system has operated steadily, and the process from issuance to transaction and circulation was realized automatically. In addition, blockchain, as a fundamental support technology, has gradually become independent and been applied to more scenarios. Based on blockchain, a variety of digital currencies come into being, such as Litecoint, Dogecoin, Ripple and so on.

In 2015, as the Ethereum open-source project brought about the concept of smart contract platform, a variety of assets and contracts were registered and transferred, which facilitated the issuance and circulation of digital currencies, and enriched the digital currencies. Especially from early 2017, various digital currencies, by means of ICO, have emerged one after another, thus making the digital currency market flourish again. Up to December 2017, according to the statistics by Coinmarketcap, there were almost 1,000 kinds of digital currencies available, with the total market value over 300 billion dollars.

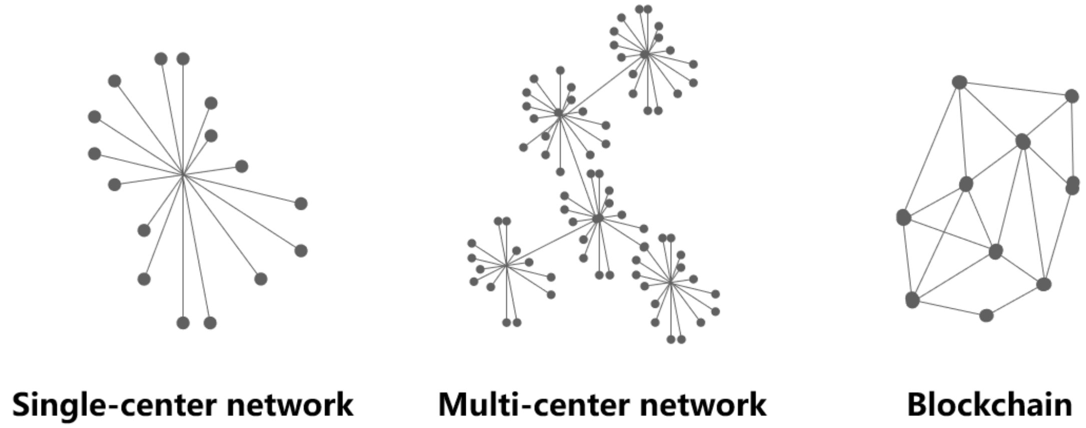
Solving the problems of valued transmission and decentralization, blockchain is praised as the most subversive technological innovation since the Internet was invented, and even the next generation of “value Internet”. Currently, more and more enterprises, after perceiving the powerful energy contained in the blockchain, are actively arranging the industrial layout, thus enabling blockchain to find commercial application in more and more industries and fields.

In our opinion, by relying on the decentralization, anti-tampering and high transparency characteristics, the blockchain technology will become another technology that innovates human society after the PC Internet and mobile Internetin this era of rapid economic development. Besides, it will be easier for people to trust various social relationships.

1.2 Features of the Blockchain Technology

1.2.1 Decentralization

In the traditional centralized network, the whole system may be destroyed once a single central node is attacked. In contrast, in the decentralized network, distributed record, distributed storage and point-to-point communication are achieved. Any node is equal to other nodes in right and obligation. The data blocks of the system will be jointly maintained by all the nodes. In this way, the whole system will still keep running normally, even though a node is controlled by an individual or organization or attacked, or stops running.



1.2.2De-trust

In the blockchain system, transaction can be conducted between nodes in the absence of trust, for the reason that the rules for system operation are made open and transparent, all the data are open and all the nodes operate according to the same transaction rule.

This rule is based on consensus algorithm instead of trust. Therefore, within the rules and time designated by the system, a node cannot cheat other nodes, so the involvement of any third party is not required.

1.2.3 Being Unalterable and Encrypted

The hash algorithm for the blockchain technology is able to correspond any original data, picture or music, to a specific figure and turn it into a hash value. Once a node is maliciously tampered, its hash value will change, which can be easily identified.

Hence, once data is verified and stored in the blockchain, it is invalid to modify the database from a single node, unless 51% of the nodes in the system have been controlled simultaneously. If a node wants to change the confirmed result, the price it pays will be much higher than the return it gets. In a word, the blockchain achieves a very high data stability and reliability.

1.3 Update and Iteration of Blockchain Network

Blockchain has opened a new era of asset management. It is the first time that people can get back their management right of their own assets, see how the asset is allocated and save the economy from the control of a few people.

However, in the booming application scenarios, there are some improper parts, in which the more notable problems include insufficient transaction volume, too slow confirmation and higher transaction charges. Because Bitcoin network is distributed highly, it is not feasible to repair the existing key problems. Thus, people tend to create new projects, but not keep repairing the original Bitcoin projects, so as to solve these problems.

Then, in recent years, people have invented Ethereum, EOS, Monero, Stellar, Cardano and other Blockchain projects. Almost all of them aim at overcoming the existing issues of Bitcoin and adding some new features, but have not solved those inconveniences for the original Bitcoin. Besides, no profits can be achieved among these projects.

Fortunately, some Bitcoin believers choose to repair the Bitcoin network itself. They have also proposed many good solutions. Lightening Network, a micro payment system established in the original Bitcoin network, is the most excellent among them. It does not need to change the code of Bitcoin. Another interesting scheme comes from the Liquid project of Blockstream, which is the sidechain of Bitcoin network.

All of these trials have pushed forward the innovation of the whole Bitcoin technology. Besides, the original security of Bitcoin network and its distribution feature are not sacrificed. The similar technology has appeared among some Bitcoin competitors very quickly, such as Raiden Network on the Ethereum.

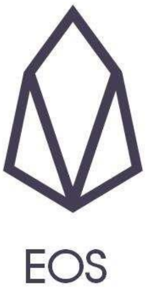
1.4 Common Public Blockchains and Their Characteristics

1.4.1 Ethereum

Ethereum is an open source public blockchain platform with smart contract function. Peer-to-peer contracts are processed by providing a decentralized virtual machine (known as “Ethereum Virtual Machine”) through its dedicated encrypted currency "Ether".

The concept of Ethereum was first proposed by programmer Vitalik Butrin from 2013 to 2014 after being inspired by Bitcoin, to the effect that “the next generation of encrypted currency and decentralized application platform”, which was able to develop through ICO crowd-funding in 2014. As of June 2018, ETH is the second most valuable encrypted currency, and Ethereum is also known as the “second generation of blockchain platform”, second only to Bitcoin.

1.4.2 EOS



EOS can be understood as Enterprise Operation System, namely a blockchain operating system designed for commercial distributed applications. EOS is a new blockchain architecture introduced by EOS software, which aims to realize the performance expansion of distributed applications. Notably, it is not a currency like Bitcoin and Ethereum, but a token issued for EOS software projects, which is called blockchain 3.0.

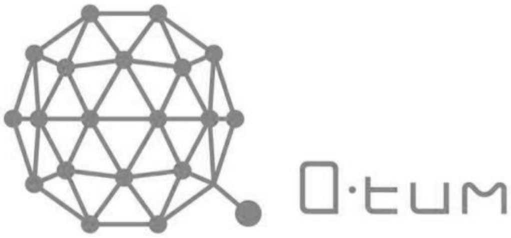
The main features of EOS are as follows:

●EOS is somewhat similar to the windows platform of Microsoft. It supports the parallel running of multiple applications at the same time by creating a blockchain underlying platform that is friendly to developers and provides an underlying template for dAPP development.

●EOS solves the problems of delay and data throughput through the parallel chain and DPOS. EOS is capable of processing thousands of transactions per second, while bitcoin can only process about 7 transactions per second, and Ethereum can process 30 to 40 transactions per second;

●EOS is free of service charge and has a wider ordinary audience. For the dApp development on EOS, the network and computing resources needed are allocated according to the proportion of EOS owned by developers. If you own EOS, it is equivalent to having computer resources. With the development of DAPP, you can lease the EOS in your hand to others for use. From this point alone, EOS also has extensive values. In simple terms, if you own EOS, it is equivalent to owning a house for you to collect rent from others, or owning a land for you to lease to others for house-building.

1.4.3 Qtum



Qtum combines the advantages of Bitcoin ecology, and is perfectly compatible with all kinds of virtual machines including Ethereum through the account abstraction layer (AAL), and adopts the Proof of Stake (PoS)Mechanism, thus providing unlimited possibilities for implementation of commercial applications and distributed mobile applications. However, problems inherent in PoS mechanism still exist. Without specialization, participants with equity do not necessarily hope to participate in bookkeeping; bifurcation is easy to occur and needs to wait for multiple confirmations. There will never be finality, which requires the checkpoint mechanism to make it up.

1.4.4 ONT

Ontology Network is the first basic platform in the world to propose a distributed chain network system. In addition to the realization of blockchain systems under different governance modes supported by the distributed account book framework of ontology network itself, it can also cooperate with different chains from different business fields and different regions through various protocols of ontology network, so as to form cross-chain and cross-system interactive mapping of various heterogeneous blockchains and traditional information systems. Therefore, Ontology Network innovatively proposes a matrix three-dimensional grid architecture, namely hyper-converged chain network structure.

1.4.5 ETP

Metaverse

Metaverse is a decentralized public blockchain project. The technical framework of Metaverse ecology includes smart property, digital identity (avatar) and value intermediary (oracle). The project will support communities to develop various financial and life apps based on the smart property on its public blockchain. Metaverse project was developed and maintained by View team in the early stage. When the project reaches a certain maturity, its code will be published on github, while View team will develop baas platform on the Metaverse blockchain to provide technical and business support services for enterprise users. Individual technologists can engage in the development and provision of games and generate game competition to improve the prime number of games.

1.4.6 NEO

The consensus mechanism of NEO is DBFT, which is the abbreviation of Delegated Byzantine Fault Tolerant. DBFT provides fault tolerance for a consensus system composed of n consensus nodes. Such fault tolerance includes both security and availability, which can resist common faults and Byzantine faults, and is applicable to any network environment. Under the DBFT consensus mechanism ofNEO, a block is generated every 20 seconds or so, and the transaction throughput can reach about1,000tps upon test, suggesting excellent performance in the public blockchain. With the appropriate optimization, there should be a chance to reach10,000TPS, which can support large-scale commercial applications.

1.5 Prominent Pain Points of Public Blockchain

Although after the development of a decade or so, there are still many prominent pain points in the mainstream public blockchain system in the current market, which are mainly reflected in the two aspects of technology and industrial implementation:

1.5.1 From a technical perspective

(1) Limited scalability

At present, all public blockchain consensus mechanisms share a fatal weakness: every node must participate in every transaction. Accordingly, each node in the network is obliged to participate in each transaction and protect the system by saving a copy of the entire transaction. Decentralization limits the number of transactions that can be processed by the blockchain, thus limiting the number of all nodes in the network, which will lose part of the scalability.

(2) Low processing efficiency

Mainly reflected in two aspects:

a) Low throughput: the transaction processing capacity of the blockchain is limited;

b) Slow transaction processing: transaction processing takes a long time. For example, bitcoin takes 10 minutes to generate a block, while it is 14 seconds for Ethereum. At peak times, Bitcoin takes longer to process a transaction. Bitcoin does not show any advantage over time of using Square or Visa.

(3) Insufficient storage capacity

Most applications built on the public blockchain require certain storage solution. (User identity, financial information, etc.).

However, storing information in a public blockchain database means that the data is:

1) Stored by each full node in the network.

2) Stored indefinitely as the blockchain database can only be added and cannot be revoked.

Therefore, data storage brings huge load to the distributed network, and every node must store more and more data. Therefore, storage is still a big problem for decentralized applications.

(4) Threat of double-spending

Double payment (also known as double-spending) is a conception of failure mode of digital currency, that is, the same digital cash can be spent more than twice. Unlike the physical symbolic currencies such as coins, electronic documents can be copied, so the behavior of spending does not remove the state of ownership from the original holder, i.e. the amount of money that has been paid but not removed becomes surplus without foundation, or the payee is enabled to receive amount of multi-payment out of the void, just like counterfeit currency, causing inflation and currency devaluation, thus making people no longer trusted and willing to hold for circulation.

In May 2018, BTG, the then 26th encrypted currency, was attacked by 51% double-spending, which was the first time that the blockchain had been tampered with. The attacker stole more than 388,200 BTGs from the exchange, with a worth as much as US$ 18.6 million.

In January 2019, ETC was attacked by double-spending. Gate Research Institute issued a notice saying that it confirmed that Ethereum Classic (ETC) network suffered 51% attacks and located the ETC address of the attacker. In this attack, Gate detected a total of 7 rollback transactions. Four of them, totaling 54,200ETCs, came from the masterminded attackers.

Hackers with 51% of the computing power of the whole network can regain the spent digital assets to their own accounts. In addition, since a transaction record has a time window from its generation to its linking to the blockchain, hackers can take advantage of such “time difference”. In fact, double-spending is a fraud that uses the time difference confirmed in the block.

1.5.2 From an industrial perspective

(1) Limited application of technology

Lacking a new type of smart contract platform and the connection with the real society, the wide application of various industries is limited and cannot be relieved in a short period of time.

(2) Long development cycle with great difficulty

Blockchain is a combination of various technologies, which requires higher capabilities of developers, while the technical talents of blockchain are scarce; blockchain technology is still in its early stage of development, and there is neither mature underlying framework and modulesthat can be directly used, nor a set of technical standards that can be followed, and communication between different chains is impossible, which leads to some problems of the blockchainsuch as long development cycle and great development difficulty .

(3) Lack of interaction with the real world

The existing blockchain system shows great closeness. At present, most smart contracts only accept data on-chain as trigger conditions, and lack interaction with the real world. The requirements for consensus mechanism are different due to the different participants.

1.5.3 From a financial perspective

Bitcoin, as a kind of “digital gold” and “virtual gold” , is featured with strong monetary attribute and represents a new monetary system, but it is quite difficult to become a common currency and payment currency. The design concept and monetary system of Bitcoin seriously violate the basic attributes, operating rules and value logic of currency.

1.6 Liberum arises at the right time

In order to solve these problems and promote the actual commercial application of the blockchain, we hope that we can combine the underlying technology of the blockchain, the value network thinking and the commercial operation system of the blockchain, so as to create a brand-new ecological circle that can solve all-round and full-cycle value circulation of the global community.

Liberum arises at the right time.

As a global future internet value transmission protocol, Liberum is a completely new blockchain ecosystem which drives the development of the entire blockchain industry.

This White Paper will describe a groundbreaking solution that combines the best practices of existing blockchain with new scalable group chain technologies, with a view to significantly advancing the smart contract performance. The technologies described in this White Paper are no longer the pure theoretical discussion on paper, but the actual and real technology that has been developed, tested and will soon be put into production.

Chapter II

Introduction to the Liberum Project

Chapter II. Introduction to the Liberum Project

2.1 What is Liberum?

The Liberum program aims to provide a scalable and resilient blockchain that supports digital asset transactions, data access, and process control through a layered structure. It creates a framework that allows users to execute smart contracts in an efficient manner. Also, it provides a developed architecture that uses the underlying infrastructure to quickly and easily generate subchains. What’s more, it is a blockchain platform that provides necessary components for the construction of sub-chains, and provides solutions for the testing of new ideas, the deployment of private chains, the processing of complex tasks, and the application of smart contracts.

With the mutual coordination, circulation and balance of its transparent and public information, smart contract-based conversion, cloud node, distributed Liberum transaction, super node, new currency circulation and unique smart contract function, the powerful internal structure of Liberum is formed in the the initial stage. All of its inherent financial balance, community promotion, business connection, value deposit and network expansion will subvert the concept behind the centralized business model. Finally, Liberum will become a commercial finance cloud network source to be used all around the world. In this open network, the joint efforts of community will be made to create a brand-new and decentralized business freedom cloud node.

What Liberum brings is not only a new blockchain product, but more importantly, it brings a completely decentralized financial cloud system and a truly subversive commercial financial practice. By relying on the unparalleled cloud logic of business finance, Liberum will show the preciousness of a system of excellence that is superior to any business model seen by the public.

2.2 Vision of Liberum

From the technical perspective, Liberum will become the “Mother of All Chains”, providing chain issuance services for all walks of life. Its core value is to technically solve the processing speed, state storage and external environment required by blockchain applications, including other subchains and external blockchains, and even cross-chain technical issues between other networks.

From the industrial perspective, Liberum provides underlying technological support for the development of the blockchain industry through Liberum, cross-chain technology and smart contracts, so that developers and enterprises can quickly use the blockchain to achieve their own business and promote the implementation of blockchain business applications. In addition, it enables people to enjoy the security, transparency and convenience brought by blockchain faster, and promotes the society into a new era.

From the financial perspective, Liberum will create a distributed trust for the future where everyone can issue blockchains and all users mayrealize self-finance. By usingthe enhanced blockchain technology and innovative applications, it will subvert the current bottleneck encountered by the blockchain industry, achieve the breakthrough development, and lead the construction of the blockchain industry ecosystem. Liberum protects the interests of all participants through blockchain technology, promotes the entire ecological data on-chain, receives maintenance from multiple parties, breaks the barriers of traditional value circulation, improves the efficiency of value transmission, establishes a free, equal, secure, credible, open and shared industry ecology and builds a new situation.

We will give full play to the powerful force of global star team, join hands with high-quality investors and consultants, and invest 100% of our passion and resources in achieving our vision and goals with our core matchmaking technologies that are overwhelmingly superior and mature products.

2.3 Mission of Liberum

2.3.1 Providing a flexible and simple blockchain infrastructure

Liberum provides a variety of modules for developers and users. Without studying the underlying technology details such as cryptography, consensus mechanism and storage method, the developers and users may directly select the required modules from the module warehouse of the chain factory and configure parameters according to their business, and quickly build a blockchain, thereby reducing the commercial cost of blockchain.

2.3.2 Supporting massive blockchain application scenarios

At the application level, it can be expected that blockchain applications will gradually enter the work and life of institutions and even individuals. Liberum provides the ability to quickly build chains through modularity, the ability to circulate data and assets between different blockchains through cross-chain technology, and Turing complete programmability through the smart contract. Therefore, Liberum can support a variety of future application scenarios.

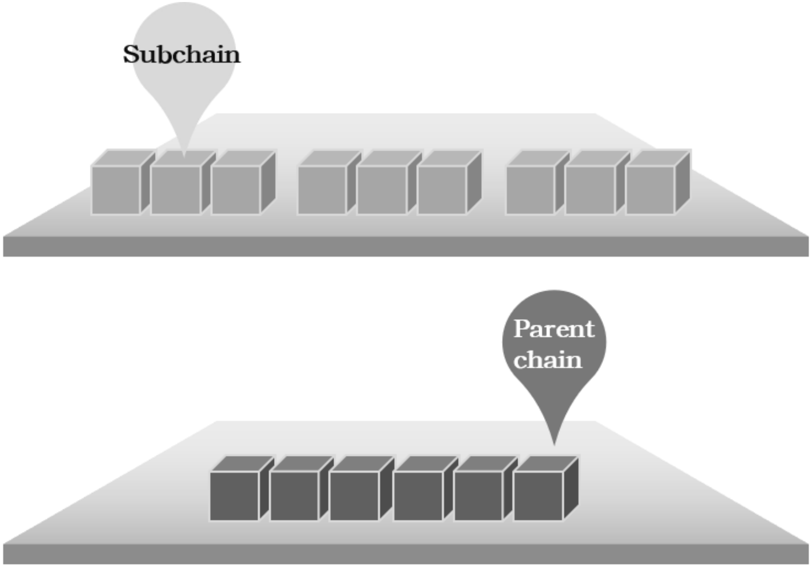
2.3.3 Drivingthe commercial landing of blockchain

Commercial applications have extremely high performance requirements, and Liberum is committed to solving the performance limitations of existing blockchains. It uses parallel expansion technology, and builds multiple independent chains through a chain factory and distributes business to each chain, so that the chains communicate through cross-chain technology to meet the needs of ten million level TPS.

2.4 What Is Liberum's Subchain

Subchain refers to the blockchain that has independent functions and it is derived from the platform of the parent chain. However, a subchain cannot exist on its own. It must provide infrastructure through the parent chain to operate. Liberum subchain is characterized by low cost, decentralization, security and high efficiency.

Subchain can be seen as a service. In this way, one subchain can serve other subchains; on this basis, the numerous subchains on Liberum are equivalent to the whole, and users can use these multiple blockchains to build a powerful application.

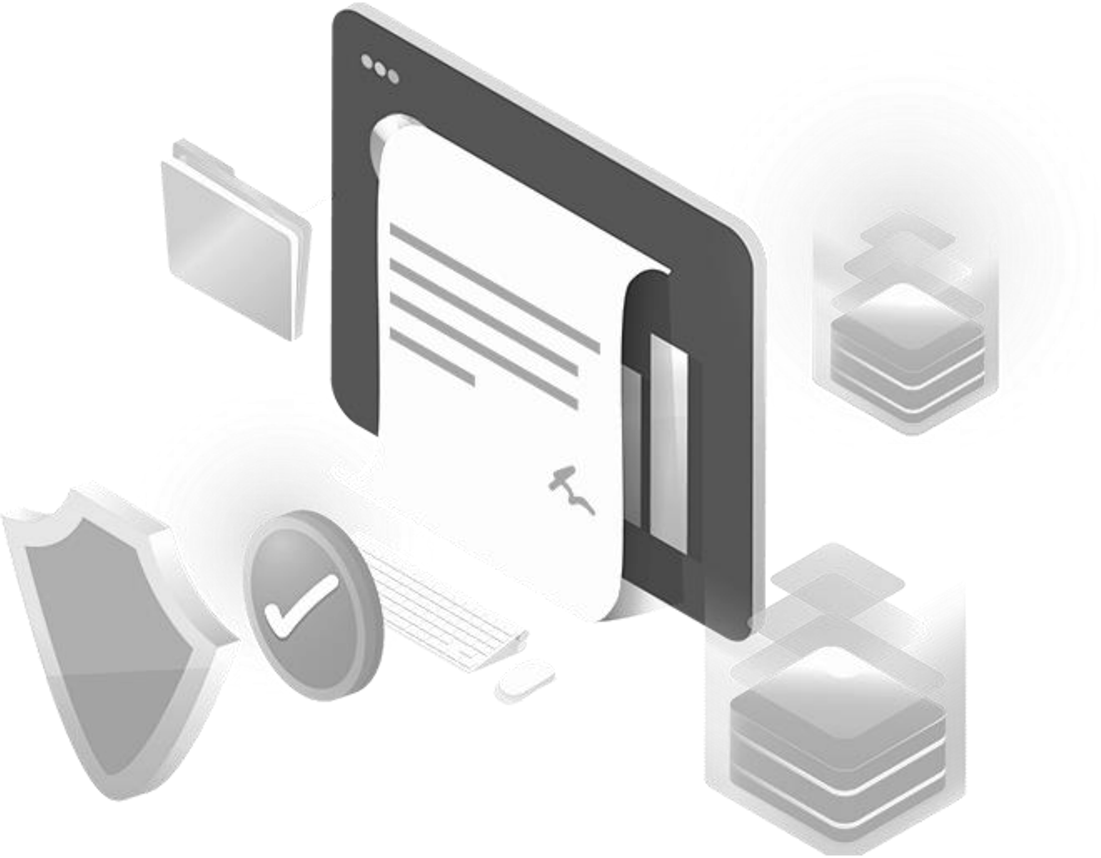


The Liberum public blockchain processes tasks separately by using subchains, and provides blockchain functions separated from business logic for each individual smart contract. By providing a separate subchain for each smart contract, it enables the smart contract to customize the consensus mechanism and have more extensive application scenarios under the potential business logic.

Developers are free to choose the consensus mechanism that best suits their business scenarios, and autonomously determine the number of subchain nodes allocated to a particular smart contract. All states of the smart contract are saved in the local subchain, and data can be written to the main chain as needed.

A subchain cannot exist alone. It must run through the infrastructure provided by the main chain, and get all users of the main chain for free. Unlike the parallel operation of side chain and main chain, the Liberum subchain and the main chain are concentric with each other; if the subchain is attacked alone, it will have no effect; the Liberum main chain uses tens of thousands of nodes and the long-tested POW consensus mechanism, and its security is very stable. While Liberum subchain obtains all users of the main chain for free, its security is also protected by the main chain. Subchain usually only needs to select a small number of nodes, such as a hundred nodes. According to statistics, the security they can achieve is the same as that of selecting all tens of thousands of nodes, which can be achieved by selecting a small number of nodes through subchain; this degree of parallelism can be one hundred, one thousand or even ten thousand, depending on the number of nodes that can provide services.

The technical path of subchain not only solves the security problem of side chain, but also provides a series of powerful functions.



2.5 Reasons for Using the Liberum Subchain

2.5.1 Subchain achieves the scalability of the blockchain system

It is very difficult to solve the sharding on a single blockchain, and the Liberum blockchain uses subchain to achieve sharding perfectly.

For a smart contract, we deploy it as a subchain; we only save the state ofcontract within the subchain, and do not need to store contract application specific information on the main chain, which greatly eases the storage pressure of the main chain. Meanwhile, the realization of high-parallel processing through the subchain may greatly ease the processing bottleneck of the main chain.

2.5.2 The subchain provides great flexibility

Liberum subchain has its own incentive mechanism, and its nodes are randomly selected from the Liberum public mining pool. In this way, while many enterprises avoid the huge cost of deploying and maintaining nodes, Liberum effectively guarantees the security of the blockchain. With only a small amount of maintenance costs, the project party may easily implement user chaining, commodity chaining, institutional chaining and process chaining. This brings the following advantages:

(1) Flexibility of consensus method

The consensus method of a single blockchain is fixed after the deployment is complete. For example, the Bitcoin consensus method is POW;when an application (DAPP) is deployed on this basis, other consensus methods should not be selected.

If the fast POS consensus method is preferred under new application scenarios, this problem cannot be solvedbecause the consensus method of the underlying public chain has been fixed. However, the subchain function of the Liberum blockchain can select different consensus modules according to the needs of the DAPP; in addition to the basic consensus methods currently provided by the system (POW, POS, PBFT, IPFS and DPOS), it also supports customized writing of new consensus methods .

In addition, the block generation speed on the subchain is not limited by the public chain. It exists independently. The users may customize the block generation speed at 10 seconds, several minutes or even an hour.

(2) Flexibility in fees

Subchain can be deployed according to different application scenarios and no longer charge a fee when calling subchain functions. This greatly reduces the threshold for users to use DAPP, and allows mass users to use DAPP conveniently and quickly and to experience the benefits brought by blockchain technology, instead that the current blockchain applications can only be limited to cryptocurrency enthusiasts.

2.5.3 Easy cross-chain to realize the interconnection of all

things

The subchain function of the Liberum blockchain can realize cross-chain transactions between the Liberum chain and other blockchains, such as between Liberum and Ethereum, between Liberum and Bitcoin; in a broader sense, it can realize the communication between the blockchain and other networks, such as the cross-chain of the Liberum blockchain and the IPFS decentralized file storage network.

2.5.4 Subchain services make powerful functions and complex DAPP possible

Subchain can not only be used as a support platform for DAPP, but also be deployed as a public service for providing other subchains or DAPP with specific services.

These services can be decentralized file storage, completelyrandom number generator or professional processing functions, such as deep learning for AI services. Under the support of various subchain services, it can build powerful DAPPs or decentralized cloud services. Such a revolutionary application model will shake the existing cloud operation methods andbring profound effects.

2.6 Comparison with Other Public Blockchains

2.6.1 Service quality

Compared with other platforms, DApps can run more efficiently on the Liberum public chain. Limited by scalability and transaction processing per second, Ethereum itself cannot handle large transactions and high concurrency. This is why a game as simple as CryptoKitties can cause congestion throughout the Ethereum network. Similar blockages caused by running 10 or 100 applications on Ethereum simultaneously could be even more catastrophic.

2.6.2 Cost

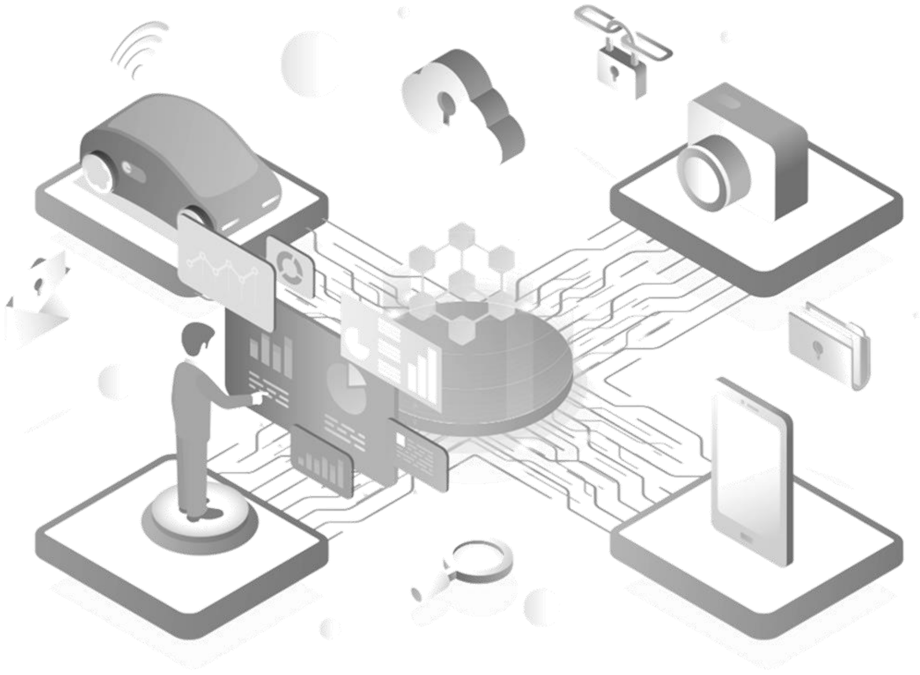
The cost of running a smart contract or DApp on Ethereum is very high. Each transaction initiated or triggered by a smart contract requires a certain amount of gas. The average gas per transaction is very high, implying that the cost of each transaction is very high. If certain smart contracts trigger many transactions, this indicates that the developer or user of the smart contract must pay a large amount of currency, cryptocurrency or other costs for the purpose of maintaining DApp.

The underlying GAS cost of the Liberum public chain is one-tenth the cost of Ethereum, while the interaction of the upper-level subchain contract is free.

2.6.3 Flexibility and simplicity

Most DApps only have their own trading logic in Ethereum. However, the remaining logic and components are “off-chain” solutions; they rely on traditional servers and databases to make them a centralized system. In contrast, DApps deployed on the Liberum public chain still maintain truly decentralized. Liberum also provides upper-level subchains for CPU computing, GPU computing, file storage, databases and many other services, while maintaining a decentralized structure.

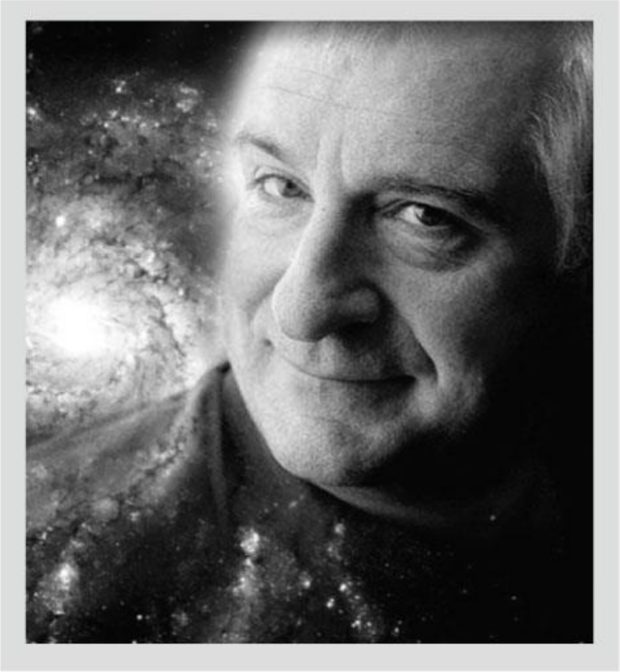
The Liberum public chain provides developers and their smart contracts with a truly scalable ecosystem. For developers, if a DApp is created in the Liberum public chain, it will have lower operating costs, more platform features and better performance under the premise of guaranteed security.



LIBERUM

Chapter III

Technology Innovation System of Liberum



“We are stuck with technology when what we really want is just stuff that works.

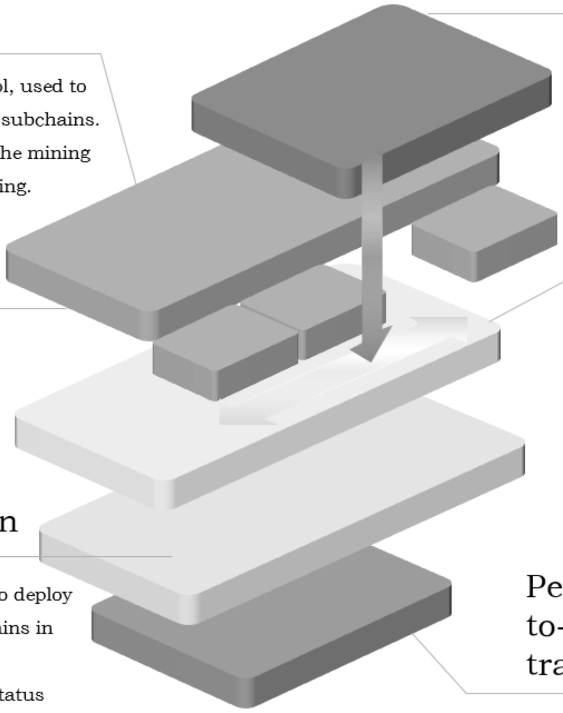
—— (Douglas Adams)”

Chapter III. Technology Innovation System of Liberum

3.1 Public Blockchain of Liberum

Liberum is designed to have a flexible blockchain structure made up by the parent chain and the subchain. The parent chain is responsible for the basic transactions and the transfer of payment, while the subchain is responsible for performing the smart contract and implementing the applications and services in varied scenarios. The design of flexible side chain enables different industries, different applications and different services to be deployed on different side chains, so as to satisfy the diverse value demands.

With an advanced layered chain-group system, and by separating transactions from smart contract, Liberum achieves a speed 100 times faster than Ethereum in transaction processing. The architecture of Liberum system is shown as follows, including fundamental chain, event processing system, technology of performing smart contract through sub-chain, fragmentation technology, cross-chain technology, safety performance, API and so on.



Upper subchain and smart contract

This is a Liberum-based protocol, used to specify the way of consensus in subchains. It is allowed to be registered in the mining pool nodes to participate in mining.

API

It achieves the convenient access of blockchain functions.

Intelligent logic

Smart contract request

Event processing

Transactions are verified by means of consensus system, validation and event processing.

Global parent chain

It is a blockchain system used to deploy and control a number of subchains in the bottom layer. It provides information such as subchain status refreshing, miner rewarding and subchain node punishment.

Peer-2-Peer (Peer-to-peer transmission)

This is the communication layer used to transmit the account transactions between nodes and the DAPP data.

3.2 Parent Chain: HWD-PoW Innovative Consensus Mechanism

3.2.1 Introduction to unique HWD-PoWinnovative mechanism of Liberum

On the public blockchain of Liberum, the parent chain is a public blockchain layer used to process transactions, operations of other blockchains, consensus and data access. Liberum also supports the use of subchains to implement other consensus algorithms.

Proof-of-Work (PoW) algorithm is an effective measure. It is able to prevent and finally prohibit the third-party interference, including denial of service attack, other services and Internet abuse (such as spam mails). PoW requires service requestors to provide some proof of work, generally providing specific tasks for the computer to fulfill in given time, thus to eliminate wrong systems. However, PoW still faces the risks of double spending or 51% attack.

The unique and innovative HWD-PoW consensus mechanism of Liberum has significantly increased the costs of double spending attack and 51% attack. With this mechanism, we can, based on the miner distribution ratio in historical blocks and the total historical weight difficulty, determine whether it is necessary to switch to another branch. We made experiments in three real major networks of Ethereum, which proved that HWD-PoW plan raised the attack cost to more than 100 times higher.

Our HWD-PoW mechanism can be applied to all PoW-based blockchains. It is able to greatly enhance the security of smaller blockchains, and make them easily integrated.

3.2.2 51% attack and cost

Firstly, let’s review the scheme of 51% attack. Suppose that the current hash rate is Po, and the attacker has a higher hash rate, Pa (Pa>Po), and based on this rate works out a hidden branch Ba, double spending is caused by the attacker on two branches. Then the attacker will expose the hidden branch Ba, and invalidate all the transactions in the original branch, Bo. This is the so-called 51% attack, which will produce the following cost.

$$Cost = (P * R) * f * t \qquad (1)$$

P represents the price of token in exchange, R represents the reward of block, f represents the generation rate of block, and t represents the duration of attack. Here we make a simplified estimate of the cost. Suppose that the price of token approximates the cost of mining. For many small blockchains, it costs only several hundred or several thousand dollars to perform such attacks.

There is another element that worsens the situation. Anyone who is able to afford proper price can easily obtain hash rate. As NiceHash provides an open market for hash rate exchange, anyone can rent hash rate with cryptocurrencies to mine in target blockchain. Hence, an attacker can accumulate as much hash rate as to exceed the 51% threshold in a short time. Attackers can double-spend the tokens by means of centralized transactions, and then release the hash rate he rents and take away the profit.

3.2.3 Historical weight difficulty

We put forward a new way to improve the calculation of total difficulty of branch. This technology takes into consideration the distribution of mining addresses in the last blocks of blockchain. This protocol is referred to as historical-weight-difficulty-based proof of work (HWD-PoW). In an honest blockchain branch, miners of new blocks are probably the miners of previous blocks, and the distribution of these miners will reflect the ratio of historical mining. In contrast, in a malicious blockchain branch, the distribution of miners of new blocks is very likely controlled by attackers, which is different from the historical conventional distribution of miners. Therefore, when the historical distribution of miners is taken into consideration, people can easily separate the honest blockchain branches from the malicious ones.

Under this mechanism, branches which are less representative in previous blocks will get less weight in the calculation of total difficulty. To perform 51% attack, a malicious miner will face two choices: either to dig a longer branch, or to build his miner image in previous blocks so as to build up reputation.

Now let’s have a look at how the HWD mode defends against 51% attack.

a) Firstly, the block generation frequency of each miner is recorded in historical window period W.

$$r_i \;=\; \frac{(blocks\ mined\ by\ miner\ i)}{(total\ block\ number\ generated\ in\ window\ W)} \qquad (2)$$

Here:

$$\sum_{i=0}^{n} r_i = 1 \qquad (3)$$

b) Then each block is signed by the private key of miner. In this way, it becomes impossible for miners to forge their identities, but becomes possible to expose miners’ private key. Don’t worry, because there is a solution for this. Tokens, once mined out, will immediately be transferred from miner’s account to the cold wallet.

c) When forking is detected, the following formula will be used to calculate the historical weight difficulty (HWD) of each branch on each node.

For the only miner K in Branch B,

$$HWD_b = HWb * Db = \sum_{k=0}^{l} r_k * \sum_{k=0}^{l} d_k \qquad (4)$$

Rk is the generation frequency of block in historical window period W, Dk is the difficulty of block k, and L is the length of branch.

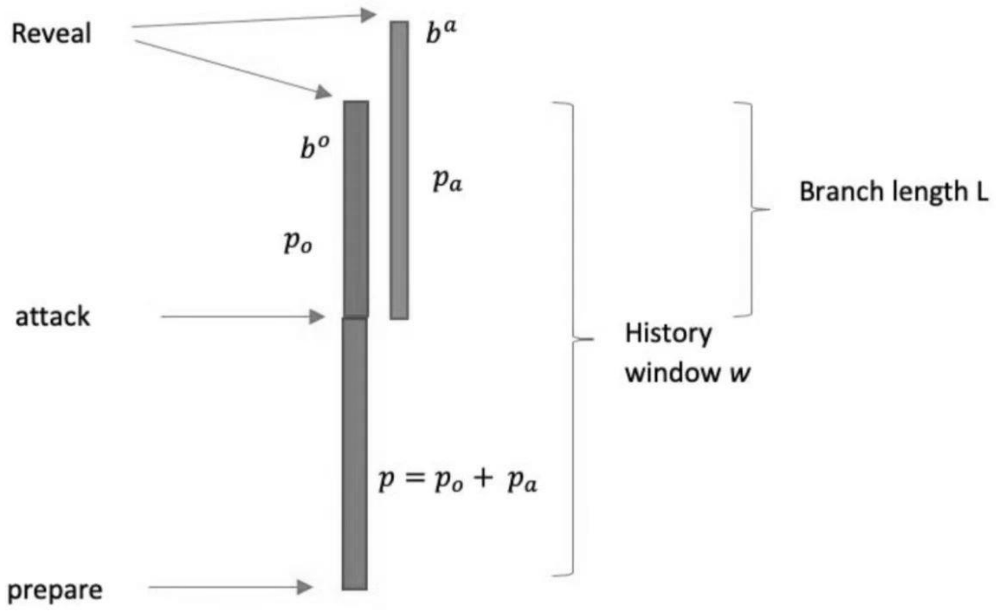
Please note that only one miner’s frequency is calculated. If one miner digs several blocks at one address, the frequency will be calculated only once. The control of single miner with high hash rate will encourage decentralized mining, thus increasing the difficulty of attack.

d) Every node will compare two different HWD values from two branches. The branch with higher HWD value will be chosen.

This mechanism has a very clear target. If the attacker adds new temporary hash rate, the miner from a new branch is new to the system, so the ri value of its block will be very low. Accordingly, the HWD will be very small, relative to the original branch. No node of the original branch will switch to the attacker’s branch. This mechanism can easily guard against the rent and attach attack.

The attacker has to produce higher HWD value if he wants to switch nodes to his malicious branch. In addition, the attacker needs to mine for some time in the original branch to include himself in history. Hence, when it switches to the hidden branch, its HWD will become higher.

Suppose Pa is the hash rate of attacker, and Po is the hash rate of the original and honest miner.



In the original branch, the attacker needs to spend hash rate Pa (The optimal spending of Pa is W/2 cycle) and time t, and then switch Pa to hidden branch at the time of attack, as shown in Fig.1. To ensure a successful attack, the following condition should be met.

$$p_a > p_o \tag{5}$$

Consequently, Ba, the malicious branch made public, will be longer than Bo, the original branch. At the time of publicity, the HWD of original branch is:

$$HWD_o = D_o * \sum_{k=0}^{l} r_k^o = D_o * (\frac{1}{2} - \delta) \tag{6}$$

In the above formula, δ is the minimum edge difference acceptable to the node. As a result, the HWD of malicious branch is:

$$HWD_a = \left(\frac{1}{2} + \delta\right) * \frac{w - l}{w} * D_a \tag{7}$$

Thus, we need to:

$$\left(\frac{1}{2}+\delta\right) * \frac{w\ -l}{w}\ * D_a > D_o * (\frac{1}{2} - \delta) \tag{8}$$

For the reason that Da and Do are approximate to each other under such condition, we can simplify the equation as follows.

$$\left(\frac{1}{2}+\delta\right) * \frac{w\ -l}{w}\ > (\frac{1}{2} - \delta) \tag{9}$$

Besides, we can reach the following conclusion.

$$\delta > \frac{l}{4w-2l} \tag{10}$$

In a word, it is the minimum cost for the attacker to spend hash rate, Po * (1/2 + l/(4W - 21)), in the time window (W - L).

For classical attack, about 50 to 500 blocks are required to cash tokens in token exchange. It can be seen from the analysis below that the switch of miner is not frequent, so we can easily set W greater than 1 to increase historical weight. When W equals to 100,000, the robustness to attack (Editor’s note: Their characteristic behaviors are maintained when the system is disturbed or becomes uncertain.) is enhanced hundredfold.

Though we cannot completely avoid 51% attack, we can increase attacker’s financial cost and time cost to more than two orders of magnitude. For the reason that it costs the attacker quite a long time to prepare for the attack, the possibility of attack becomes much lower. Long-time attack will result in substantial opportunity cost and uncertainty. Comparing with the above-mentioned HWD plan, the additional improvement plan increases the cost of attack.

3.2.4 Additional improvement plan

The above is the HWD plan. The additional improvement plan will increase attacker’s cost.

The first plan releases the upper limit for Ri < Rc. It means that the number of single miners will not exceed Rc, even though more blocks are generated in historical window. This plan will encourage more diversified mining pools. Besides, a miner can purposefully divide mining hash rate into several miners, to ensure that every miner is lower than Rc. This plan remains effective, though it steers by diversified demands. It increases the cost for attacker to maintain several miner accounts.

The second plan is to add a miner overlap demand between two forked branches. To reduce attack cost to the minimum, attackers will usually put all their hash rates in malicious branches. Overlapping demands require some miners to mine in two branches simultaneously. In this case, to achieve the switch between branches, HWD conditions should be satisfied.

$$HWD_a > HWD_o \qquad (11)$$

Besides, the degree of overlap between two groups of miners should be greater than s.

$$\{r_i\} \bigcap \{r_k\} > s \qquad (12)$$

In the above formula, Ri is the miner frequency of original branch, Rk is the miner frequency of attacker branch, and s is the overlapping threshold.

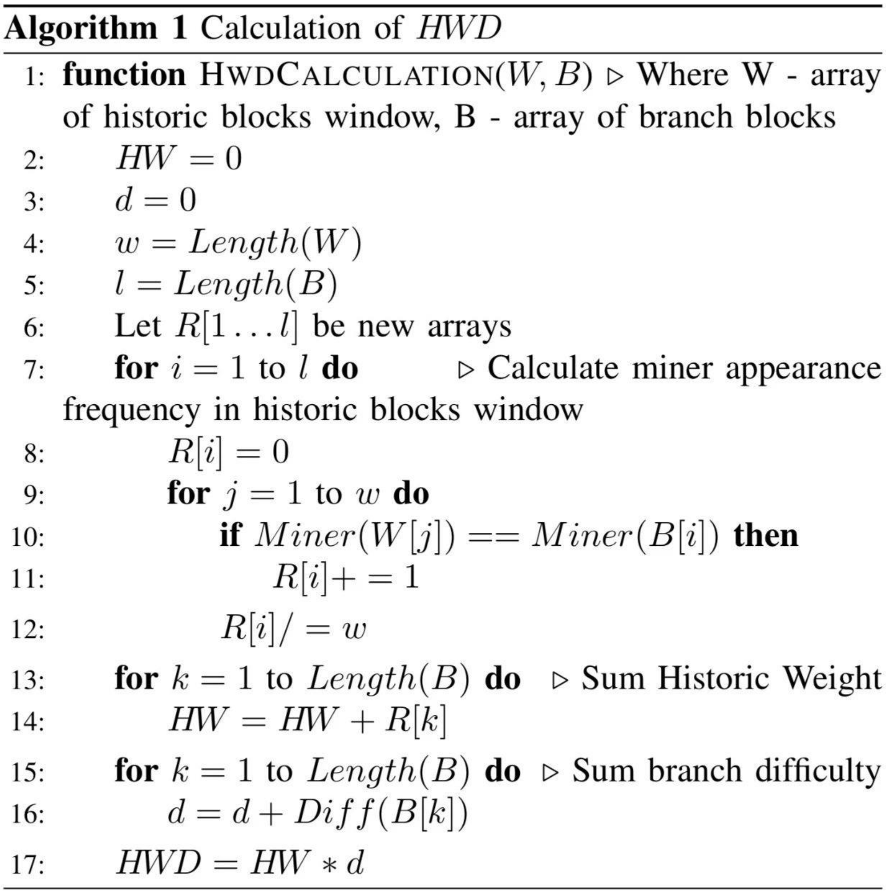
It means that the system discourages the sudden switch of hash rate from one group of miners to another group of miners.

With such an intensified requirement, and if s equals to 0.25, the attacker has to triple the current hash rate he possesses within the continuous time w. It means that the attacker has to reserve some hash rate in the original branch and reserve more than twice the hash rate in the malicious branch. Hence, by introducing such a plan, we have the time cost and financial cost for attacking original historical weight difficulty doubled and tripled respectively. For higher s value, attackers have to spend more hash rates.

3.2.5 HWD algorithm

In this section, we will introduce the branch-selection-based HWD algorithm.

The pseudocode for the calculation of HWD is shown as follows.



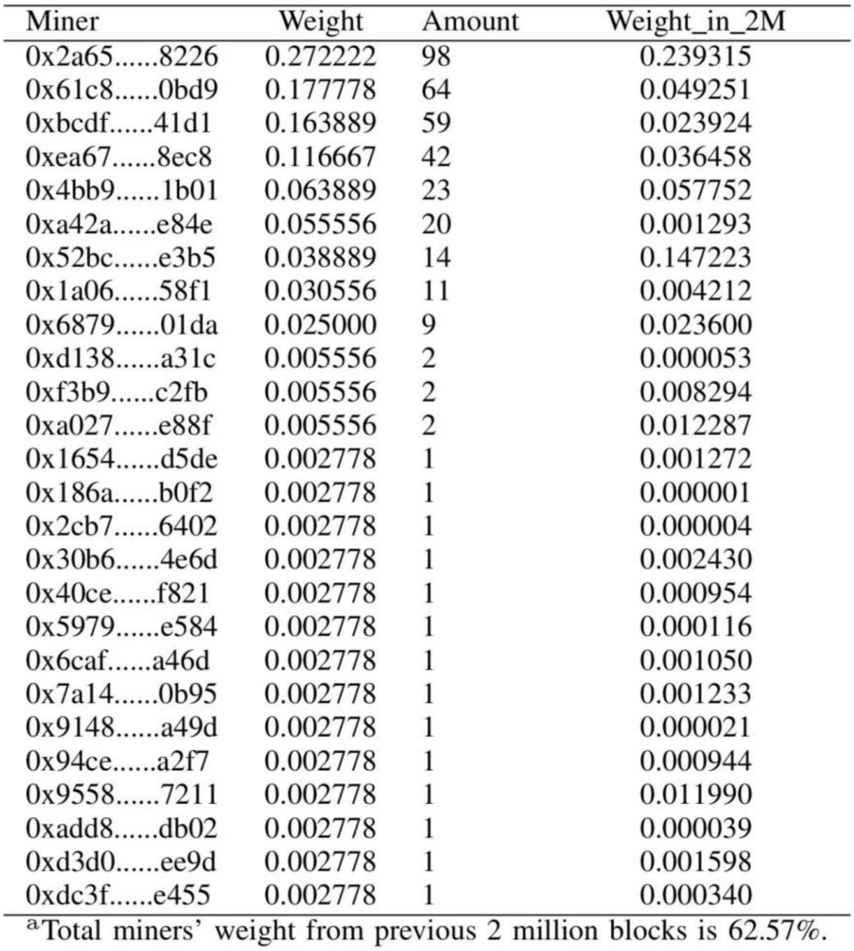
Algorithm 1 Calculation of *HWD*

```
function HWDCALCULATION($W, B$) ▷ Where W - array of historic blocks window, B - array of branch blocks
    $HW = 0$
    $d = 0$
    $w = Length(W)$
    $l = Length(B)$
    Let $R[1 \ldots l]$ be new arrays
    for $i = 1$ to $l$ do ▷ Calculate miner appearance frequency in historic blocks window
        $R[i] = 0$
        for $j = 1$ to $w$ do
            if $Miner(W[j]) == Miner(B[i])$ then
                $R[i] += 1$
        $R[i] /= w$
    for $k = 1$ to $Length(B)$ do ▷ Sum Historic Weight
        $HW = HW + R[k]$
    for $k = 1$ to $Length(B)$ do ▷ Sum branch difficulty
        $d = d + Diff(B[k])$
    $HWD = HW * d$
```

3.2.6 Real data statistics from Ethereum

We chose a famous PoW blockchain platform – Ethereum. Information of the previous 6,000,000 blocks which had been mined for about three years was analyzed. The first thing we did was to find out the distribution of miners with greater hash rate. Analysis shows that the distribution of miners is highly related to the past history. At block # 2,000,000, # 4,000,000 and #6,000,000, 360 block miners of each were analyzed respectively. The miner weights of the 360 blocks and the 2,000,000 blocks are shown as follows.

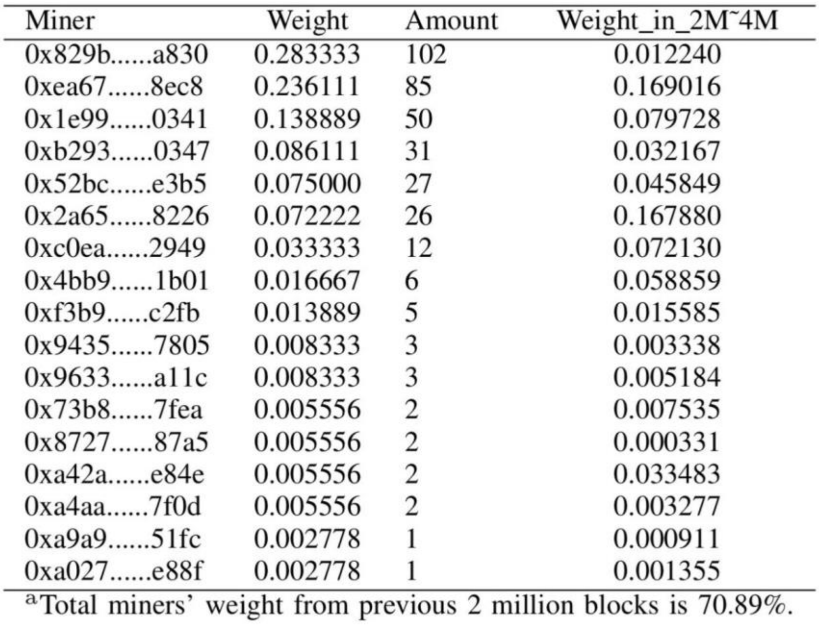
TABLE I
ETHEREUM BLOCK MINERS FROM 2,000,001 TO 2,000,360



Miner	Weight	Amount	Weight_in_2M
0x2a65......8226	0.272222	98	0.239315
0x61c8......0bd9	0.177778	64	0.049251
0xbcdf......41d1	0.163889	59	0.023924
0xea67......8ec8	0.116667	42	0.036458
0x4bb9......1b01	0.063889	23	0.057752
0xa42a......e84e	0.055556	20	0.001293
0x52bc......e3b5	0.038889	14	0.147223
0x1a06......58f1	0.030556	11	0.004212
0x6879......01da	0.025000	9	0.023600
0xd138......a31c	0.005556	2	0.000053
0xf3b9......c2fb	0.005556	2	0.008294
0xa027......e88f	0.005556	2	0.012287
0x1654......d5de	0.002778	1	0.001272
0x186a......b0f2	0.002778	1	0.000001
0x2cb7......6402	0.002778	1	0.000004
0x30b6......4e6d	0.002778	1	0.002430
0x40ce......f821	0.002778	1	0.000954
0x5979......e584	0.002778	1	0.000116
0x6caf......a46d	0.002778	1	0.001050
0x7a14......0b95	0.002778	1	0.001233
0x9148......a49d	0.002778	1	0.000021
0x94ce......a2f7	0.002778	1	0.000944
0x9558......7211	0.002778	1	0.011990
0xadd8......db02	0.002778	1	0.000039
0xd3d0......ee9d	0.002778	1	0.001598
0xdc3f......e455	0.002778	1	0.000340

[a] Total miners' weight from previous 2 million blocks is 62.57%.

TABLE II
ETHEREUM BLOCK MINERS FROM 4,000,001 TO 4,000,360



Miner	Weight	Amount	Weight_in_2M˜4M
0x829b......a830	0.283333	102	0.012240
0xea67......8ec8	0.236111	85	0.169016
0x1e99......0341	0.138889	50	0.079728
0xb293......0347	0.086111	31	0.032167
0x52bc......e3b5	0.075000	27	0.045849
0x2a65......8226	0.072222	26	0.167880
0xc0ea......2949	0.033333	12	0.072130
0x4bb9......1b01	0.016667	6	0.058859
0xf3b9......c2fb	0.013889	5	0.015585
0x9435......7805	0.008333	3	0.003338
0x9633......a11c	0.008333	3	0.005184
0x73b8......7fea	0.005556	2	0.007535
0x8727......87a5	0.005556	2	0.000331
0xa42a......e84e	0.005556	2	0.033483
0xa4aa......7f0d	0.005556	2	0.003277
0xa9a9......51fc	0.002778	1	0.000911
0xa027......e88f	0.002778	1	0.001355

[a] Total miners' weight from previous 2 million blocks is 70.89%.

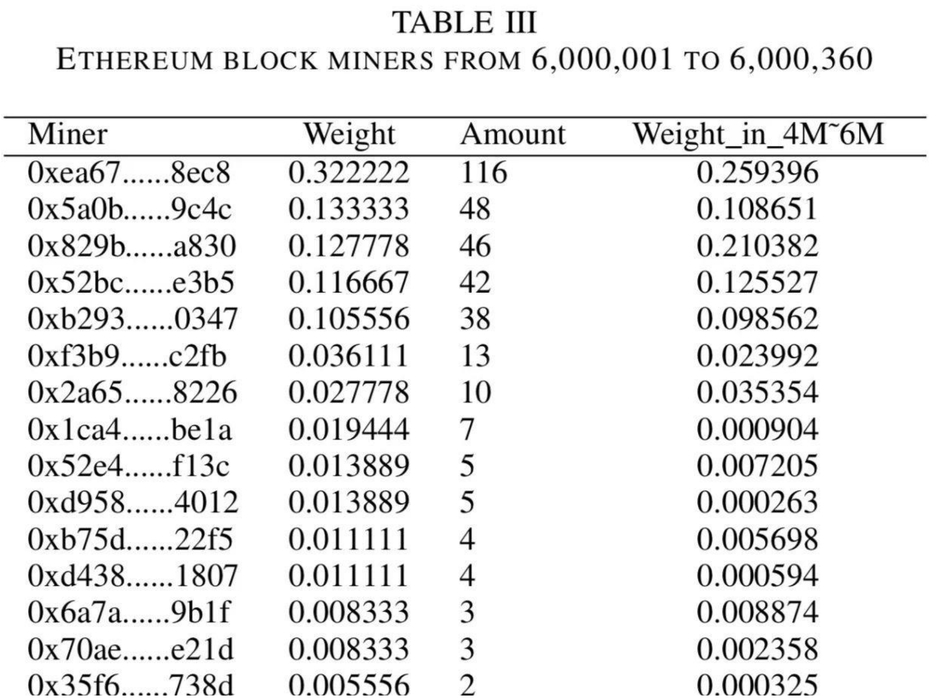


TABLE III
ETHEREUM BLOCK MINERS FROM 6,000,001 TO 6,000,360

Miner	Weight	Amount	Weight_in_4M˜6M
0xea67......8ec8	0.322222	116	0.259396
0x5a0b......9c4c	0.133333	48	0.108651
0x829b......a830	0.127778	46	0.210382
0x52bc......e3b5	0.116667	42	0.125527
0xb293......0347	0.105556	38	0.098562
0xf3b9......c2fb	0.036111	13	0.023992
0x2a65......8226	0.027778	10	0.035354
0x1ca4......be1a	0.019444	7	0.000904
0x52e4......f13c	0.013889	5	0.007205
0xd958......4012	0.013889	5	0.000263
0xb75d......22f5	0.011111	4	0.005698
0xd438......1807	0.011111	4	0.000594
0x6a7a......9b1f	0.008333	3	0.008874
0x70ae......e21d	0.008333	3	0.002358
0x35f6......738d	0.005556	2	0.000325

The total weight of miners of the 360 blocks is highly related to the distribution of historical window, even though all the 2 million (M) blocks are used (about one year). The result is shown as follows.

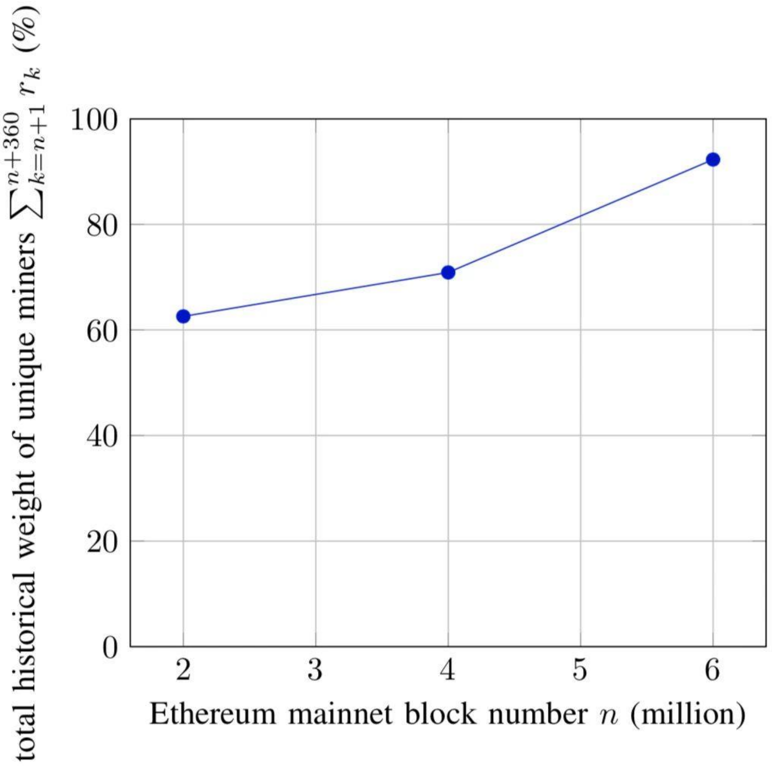


Fig. 2. Total historical weight HW of unique miners of the 360 new blocks from previous 2 million blocks.

This supports our assumption that the participation rate of honest miner is relatively stable. For this reason, the historical weight of miner is valuable information, which can be used to fight against 51% attack. It is also found out that the correlation between new miners and the previous 2 million blocks gets enhanced, showing that Ethereum mining is becoming centralized.

Please note that in table II, a miner's weight with its address being 0x829b....a830, has great changes in the 360 blocks from 2M to 4M, but the total weight of miners of the previous 2 million blocks still remains above 70%, showing that individual miners may significantly change their mining participation rate but will not change the total historical weight of a real branch.

We simulated 51% attack at block #2M, block #4M and block #6M, and monitored and calculated the results of 1M and 2M. In case the HWD of attack branch goes higher than that of original branch, the attack succeeds.

Under ideal condition, the time spent in preparations should at least be longer than the given window time. However, considering the correlation of distribution, the preparation cycle is made slightly shorter. We performed repeated simulations for each window, so as to obtain the average accumulative cost. Here we ignored the effect that mining rewards reduce by half as time goes on. The result is shown as follows.

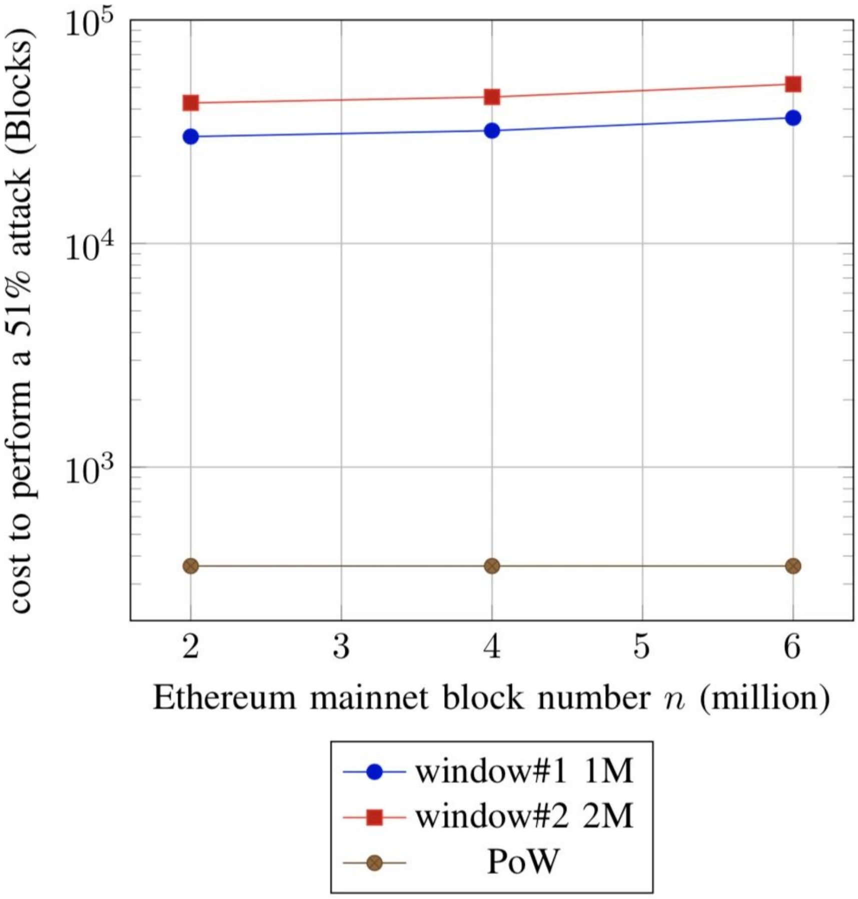


Fig. 3. Comparing the cost of perform a 51% attack, *HWD*-PoW(1M windows, 2M windows) vs. PoW

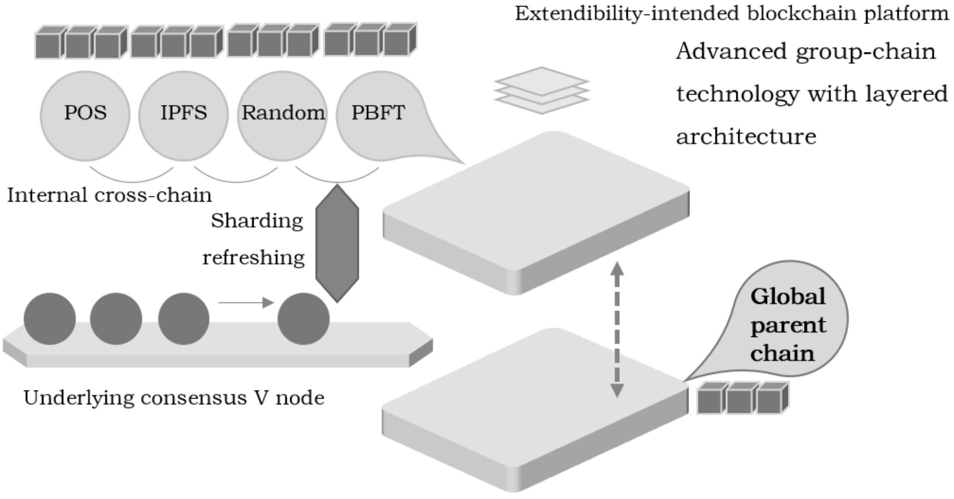
$$cost = 2 * \sqrt{window * branch\,size * correlation\,rate}$$

As suggested by the result, in HWD plan, the price of attacking Ethereum mainnet blockchain will be increased more than a hundredfold, if the size of window is set as 1M or 2M blocks. In actual application, the window can be made shorter so as to speed up the process. It is suggested that the size of window should be at least 1M, in order to increase the cost of attack more than a hundredfold.

3.3 Smart Contract Implemented in the Form of Subchain

Liberum is the first to present and implement the blockchain-based solution that each smart contract is provided with customized subchain. It comes more efficient than the existing smart-contract-performed solution, and is more extensible.

Liberum public blockchain uses subchains to implement the business logic of smart contract, thus avoiding the simultaneous handling of blockchain tasks (such as transaction consensus and records) and of the business-related logic (implemented by means of smart contract) on the same chain. By providing each smart contract with customized subchain, developers can freely choose the consensus algorithm most suitable for the application scenario, and determine the number of noes assigned to smart contract, thus to support more application scenarios. All the states of smart contract will be stored in local subchain, and data can be written into the parent chain as required.


Extendibility-intended blockchain platform
Advanced group-chain technology with layered architecture
POS
IPFS
Random
PBFT
Internal cross-chain
Sharding refreshing
Underlying consensus V node
Global parent chain

3.4 Subchain With Customizable Consensus Algorithm

Lying above the parent chain, each subchain can have its unique consensus system and algorithm.

For example, you can create a subchain that uses the PoS (Proof-of-Stake) consensus mode to achieve rapid and highly-concurrent transaction. PoS is a kind of algorithm in blockchain network, used to realize distributed consensus.

The PoS-adopted blockchain relies on verification nodes in the network to verify transactions. Unlike Proof-of-Work (PoW), it doesn't have to process mass data. In PoS consensus, creator of the next block is selected according to the stochastic algorithm of elements (stock) such as the amount of tokens held, token age and so on.

The advantage of PoS is that it can fully extend to enterprise-class transactions, offer a high efficiency, and support a variety of transactions. With the increase of nodes in the network, its verification capacity will improve accordingly. It allows DApp subchain to carry out small transactions, without having access to the parent chain continuously.

Besides Proof-of-Stake and Proof-of-Work, Liberum public blockchain also supports additional plug-and-play consensus systems, such as Proof of Activity, Proof of Burn, Proof of Elapsed Time, Proof of Capacity and so on.

3.5 Asynchronous Smart Contract

Besides the group-chain architecture, the platform also uses asynchronous smart contract and subchains to accelerate the development and deployment of DApp. This advanced architecture also extends the functions of Solidity (Ethereum programming language) and Ethereum smart contract.

Liberum public blockchain supports two types of smart contracts.

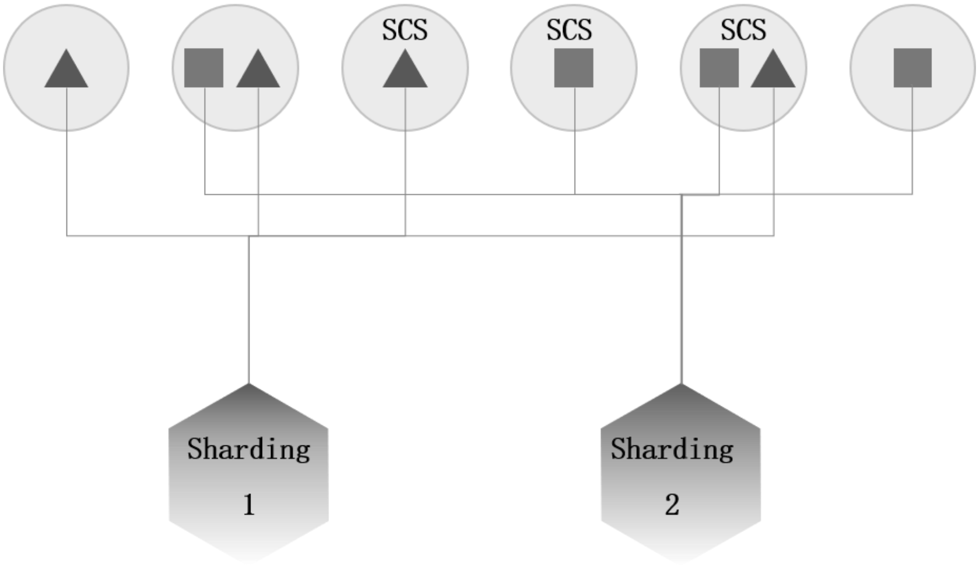
1. The subchain smart contract is protocol-based, and is used to define the consensus system of subchain. It enables nodes to register to use the mining pool.

2. The parent chain smart contract defines a variety of behaviors to control subchains, including refreshing, miner rewarding and how to punish those with misconduct. It provides a flexible environment, where DApp can use different types of virtual machines, including Ethereum, Java (JVM) and other virtual machines chosen by developers.

3.6 Blockchain Sharding

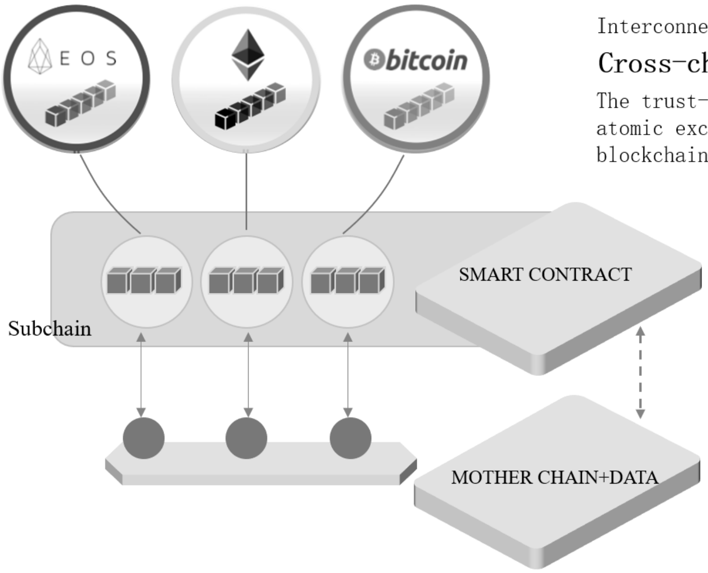
Liberum public blockchain also provides the blockchain sharding function. It is able to divide data horizontally across several blockchains and nodes. One of the causes for a low efficiency of existing blockchain solutions is that all the nodes have to process the same task many times. By sharding the nodes, this technology provides a stronger processing capacity in proportion to the number of nodes in the network.

Smaller, faster and more manageable sharding



When deploying the smart contract, developers will define the number of service nodes, consensus protocol, size of block, block generation time and refreshing frequency, which will produce divisions and provide this smart contract with Byzantine fault-tolerant solutions, thus to form subchains.

This is similar to database sharding. The difference is that blockchain sharding is a kind of blockchain subarea. It is able to divide large blockchain node into smaller, faster and more manageable sharding. In this way, Liberum can use more nodes to expand the network, thus remarkably improving TPS (transactions per second). The sharding technology divides the whole network into many divisions. As long as there are sufficient nodes in each sharding, the system will remain highly safe. The sharding technology also allows safe processing of concurrent transactions, which further increases TPS (transactions per second). Hence, it far outperforms the existing blockchain solutions.



Interconnectivity

Cross-chain ready

The trust-based system is used to achieve atomic exchange between different blockchains and between cryptocurrencies.

Cross-chain within the subchain

Achieve cross-chain communication between the parent chain and subchain and between subchains within Liberum system.

Atomic exchange

The atomic exchange with the third-party blockchain (such as Bitcoin and Ethereum) is established through the subchain.

3.7 Cross-chain Technology Is Ready

FOGS presents two cross-blockchain transaction architectures - isomorphic interchain (FOGS Orbits) and isomerous interchain (FOGS Canal), in order to achieve interconnection between independent blockchains, and to ensure the validity of cross-chain transaction and the security of user privacy and data.

As the number of blockchain users and transactions rises sharply, it becomes a mission for FOGSOrbits to solve the problems faced by the single-chain system. For instance, the trans-network consensus efficiency of the single blockchain is limited by the number of consensus nodes; the trans-network backup mechanism of the single blockchain results in a low storage efficiency; and the single-blockchain system fails to meet the diversified needs. The FOGS Orbits system has the following advantages.

(1) It supports the differentiated and diversified technical features of subchain. Different subchains can define key operating parameters of blockchain themselves.

(2) It creates subchains, provides consistency guarantee, and achieves the separated storage of subchain ledger.

(3) Integrated ledger structure of hash and index;

(4) Value can flow freely between subchains.

FOGS Canal aims to transform different blockchains from “value islands” to “interconnected systems”. In the blockchain world (with Bitcoin and ETH as the representatives), nodes only verify the transactions of their own blockchain, so independent and vertical autonomous systems are built up. Under such condition, these blockchains gradually evolve into “value islands”, and become increasingly like “local area network”, which makes it very hard to exchange assets and make communication between blockchains. FOGSCanal makes it its mission to establish an expansible and interoperable cross-chain system, thus to achieve interconnection between blockchains, transform “local area network” into “Internet”, and to achieve a free flow of value, assets and information between blockchain “value islands”.

3.8 Event Processing

Lying above the parent chain, a distributed network layer, this is an event processing system used to request and reply network events. It also handles flow-of-control requests, and calls smart-contract-related operations. Event processing system relays transaction requests in the layers of the platform in a multi-directional way. It is mainly used for transactions, global smart contract control, state refreshing, and other consensus-related information.

3.9 Mining

Mining is a process of transaction verification. In this way, new tokens are released, and awarded to miners who provide verification processing capacity and storage. Lying below the Liberum public blockchain, the PoW parent chain is the base layer for data processing and data storage. With the mining function of parent chain, Liberum miners can easily get Liberum tokens.

3.10 Wallet and Payment System

Liberum public blockchain is provided with a wallet protocol with complete functions, so Liberum can work with various third-party wallet solutions. Any wallet compatible with Liberum protocol can function smoothly on the platform.

At present, Liberum public blockchain has reached a cooperative intention with a open-source-software-based wallet, and will soon establish connections with it.

3.11 API

API of Liberum public blockchain provides DApp with user-friendly access points, and also provides DApp developers with a QuickStart channel to enable them to use specific functions of blockchain without having to know the details about blockchain implementation. It is only necessary for developers to call these functions from Liberum public blockchain to build complicated applications.

3.12 Security

Liberum puts forward a zkSNARK-based interchain transaction privacy protection method. zkSNARK, a zero-knowledge proof algorithm, is one of the relatively mature and feasible privacy protection technologies. It offers better anonymity. In addition, it neither has to trust the central node, nor needs to be participated by other users of the network. By interacting with anonymous currency, users can trade anonymously, which effectively protect the privacy of users.

To transform the transaction validation rule into the QAP form, we firstly need to transform the transaction validation rule function into the NP full-language RISC form. Firstly, the transaction validation rule is abstracted into the complex multinomial which is then decomposed into two forms: *x=y and x=y(op)z.* op can be an operator such as addition, subtraction, multiplication and division. y and z can be a variable, digit or subexpression. Secondly, the decomposed expression is transformed into a series of ternary vectors (a,b,c). Finally, the RISC form is transformed into QAP form according to the Lagrange’s interpolation. The QAP form is shown as follows.

$$\left(A_0(\chi) + \Sigma_{i=1}^{m} S_i A_j(x)\right) \cdot \left(B_0(x) + \Sigma_{\mathrm{i}=1}^{m} S_i B_i(x)\right) - \left(C_0(x) + \Sigma_{\dot{z}=-1}^{m} S_i C_i(x)\right)$$
$$= H(x) * z(x)$$

For the reason that the transaction validation rule of Interchain include the operation of the complex multinomial, such as signature verification, computation of Merkle root hash value and so on, the QAP form it structures contains a great quantity of hash functions. Directly computing the linear combinations contained in the QAP form will consume plenty of resources and time. To avoid such situation, it is necessary to transform the multinomials contained in the QAP form into the value at a certain safe random variable rn. At this time, the above QAP equation still makes sense.

The elliptic curve cryptography is needed to enable the validation nodes in the Interchain to verify the validity of transaction under the condition that they know nothing about the privacy information about the transaction such as transaction parties, transaction amount and so on. This function should satisfy the following conditions.

$$e(P, Q+R) = e(P, Q) * e(P, R)$$
$$e(P+Q, R) = e(P, R) * e(Q, R)$$

P, *Q* and *R* are the points on the elliptic curve. To verify the QAP form transformed from InterChain transaction rule, it is only necessary to verify the following equation.

$$\mathrm{e}(\delta_a \delta_b) = \mathrm{e}(\delta_c G) * \mathrm{e}\left(\delta_{h_i} \delta_z\right)$$

As the carrier to forward and verify the cross-chain anonymous transactions, Interchain should be able to verify the validity of cross-chain anonymous transactions. The cross-chain transactions are divided into the cross-chain transparent transaction and cross-chain anonymous transaction. The former provides information about the transaction itself and the related Merkle branch proof. The verification nodes of the Interchain network verifies the validity of a transaction in accordance with the verification rules for the registration of parallel blockchain. In contrast, the cross-chain anonymous transaction will not disclose any other information except the validity of such transaction. The verification nodes of the Interchain network need to learn the public parameters generated in the booting stage of each parallel blockchain network, and then use these public parameters to verify the validity of cross-chain anonymous transactions from the parallel blockchain. Zero-knowledge proof algorithm ensures that the verification nodes of the Interchain network can learn no other information except the validity of such cross-chain transaction.

> “Sense of security does not depend on what you possess, but how far you can go when you have nothing.
>
> —— Joseph Wood Krutch”

Chapter IV

Ecosystem of Liberum

Chapter IV. Ecosystem of Liberum

4.1 Basic Ecology of Liberum

At present, Liberum is building the basic ecological environment. Through a consensus incentive system, it combines distributed storage, smart contract, distributed artificial intelligence, multi-signature and other technologies to allow ecological participants to spontaneously maintain the sustainable development of the Liberum ecosystem.

Liberum is an open public basic chain that supports the development and chaining of multiple Dapps and helps all participants to participate in the ecosystem flexibly. As a result, the participants can quickly develop digital asset custody, digital asset clearing, digital asset exchange, digital index investment, asset securitization and other applications with different functions that are suitable for different player needs through technical service providers.

Liberum protects the interests of all participants through blockchain technology, promotes the entire ecological data on-chain, receives maintenance from multiple parties, breaks the barriers of traditional value circulation, improves the efficiency of value transmission, establishes a free, equal, secure, credible, open and shared industry ecology and builds a new situation.

4.2 Community

The core of the Liberum public chain is to support its users, including developers who create DApps, end users who use these DApps, and miners and node operators who keep the network up and running.

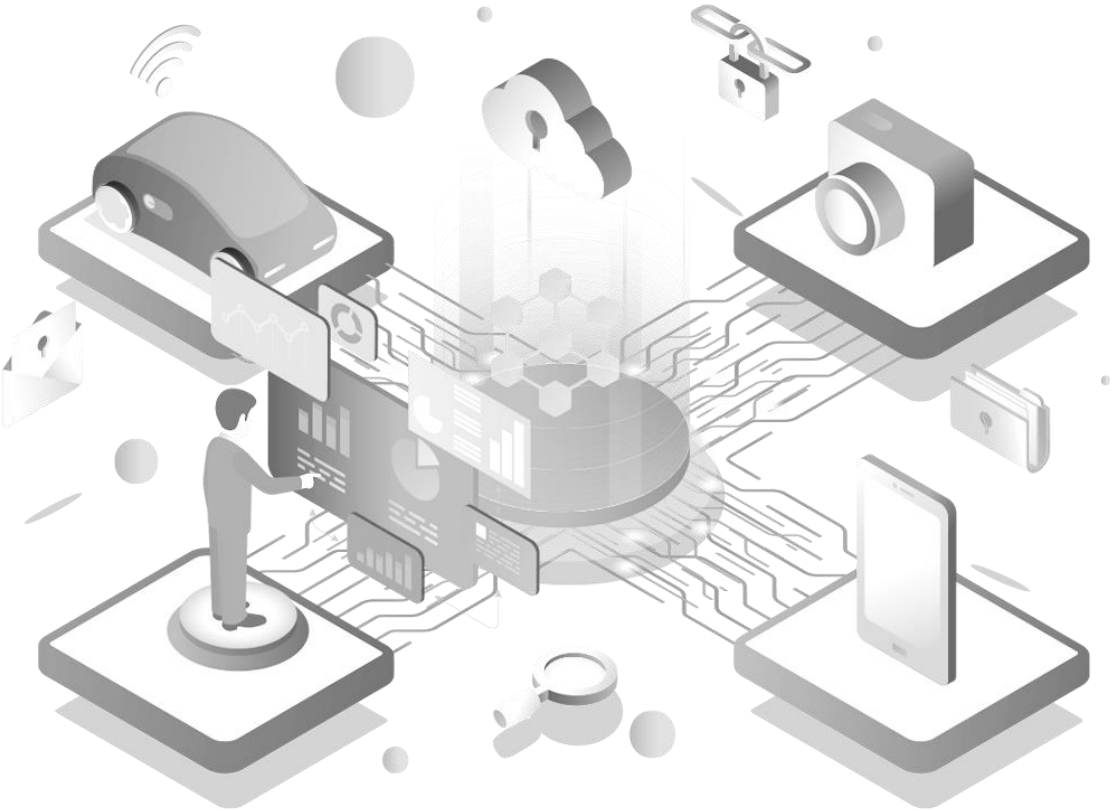
Liberum will provide a wide range of user resourses such as wikis, tutorials, glossaries, white papers, knowledge bases and help desks. Besides, it will also make active interaction with user groups on Telegram, Facebook, Twitter and other social media platforms.

Liberum public chain can be deployed in all major operating systems, such as Windows, Mac OS and Linux/UNIX. Currently, Liberum client programs are written in Golang. Of course, developers can write smart contracts in other programming languages through the provided Liberum protocol.

The community also includes DApp Labs.This function encourages developers to conduct tests and experiments, and enables developers to test DApps in isolation before publishing them to the public network.

In addition to supporting cross-chain functions interconnected with other blockchains and cryptocurrencies, Liberumpublic chain also runs on the underlying P2P distributed network. By using a P2P network, the platform may provide a distributed network for DApps to interact.

A P2P network is the underlying communication between any single or packet node running the same protocol. In this case, a node refers to a client that shares blocks and transactions on the network. The nodes communicate by sending messages using RLPx, which is an encrypted and authenticated transmission protocol.



4.3 Dividends for DAPP Developers

4.3.1 Service quality

Compared with other platforms, DApps can run more efficiently on the Liberum public chain. Limited by scalability and transaction processing per second, Ethereum itself cannot handle large transactions and high concurrency. This is why a game as simple as CryptoKitties can cause congestion throughout the Ethereum network. Similar blockages caused by running 10 or 100 applications on Ethereum simultaneously could be even more catastrophic.

4.3.2 Cost

The cost of running a smart contract or DApp on Ethereum is very high. Each transaction initiated or triggered by a smart contract requires a certain amount of gas. The average gas per transaction is very high, implying that the cost of each transaction is very high. If certain smart contracts trigger many transactions, this indicates that the developer or user of the smart contract must pay a large amount of currency, cryptocurrency or other costs for the purpose of maintaining DApp.

The underlying GAS cost of the Liberum public chain is one-tenth the cost of Ethereum, while the interaction of the upper-level subchain contract is free.

4.3.3 Flexibility and simplicity

Most DApps only have their own trading logic in Ethereum. However, the remaining logic and components are “off-chain” solutions; they rely on traditional servers and databases to make them a centralized system. In contrast, DApps deployed on the Liberum public chain still maintain truly decentralized. Liberum also provides upper-level subchains for CPU computing, GPU computing, file storage, databases and many other services, while maintaining a decentralized structure.

4.3.4 Cross-chain

At present, the Liberum public chain has implemented a blockchain platform with cross-chain functions.

Developers can now switch cryptocurrencies between specific DApps, withoutlimitation to any specific platform or technology. For example, Bitcoin, Ethereum or other cryptocurrencies may interact with the Liberum DApp, without having to switch back and forth between exchanges. If there is no Liberum, users won’t easily handle transactions between Bitcoin and Ethereum.

Unfortunately, every existing blockchain system is like an island without a bridge. Just imagine a world where every website and mobile application cannot communicate with each other through the Internet and the Internet of Things.

The Liberum cross-chain technology makes it possible to communicate between different blockchain systems. However, its potential has not yet been fully demonstrated, and larger application scenarios have yet to be developed.

4.3.5 Instant chain issuance

At present, Liberum has simplified the process of deploying a subchain into a script for instant chain issuance, which is convenient for users. As long as users select the subchain template provided by the Liberum public chain and set the subchain parameters, the usersmay complete the deployment of the subchain by using a script. As a result, the project party does not need to waste energy to develop and maintain its own blockchain, nor does it need to deploy its own node server, but only needs to pay a certain LBR to maintain the subchain operation. In this way, Liberum hopes to help project parties focus on the implementation of the logical aspects of the application, without having to spend extra effort to develop the blockchain.

4.4 Decentralized Exchange (in the closed beta test)

4.4.1 Brief Introduction to the Decentralized Exchange

Liberum Decentralized Exchangeprovides a fair, ideal and safe environment and one-stop services for investors' digital assets trading and management, release and time deposit. We will use a multi-level and multi-dimensional intelligent risk control system to ensure the transaction security of digital assets, to achieve rapid transaction and to support the data transaction in large volumes. We will use stable servers to ensure a wonderful user experience, and enable investors to trade with an easy mind instead of worrying about data security, personal information disclosure and so on. We will also meet the regulatory requirements on security, auditing, report, analysis and so on in the most secure and efficient manner, and enable all the digital assets to circulate rapidly and safely on the platform, thus to promote the better and faster development of global economic market.

As a real-time, open and transparent transaction community in the world, Liberum Decentralized Exchange does not use a traditionally centralized corporate structure, without a CEO or board of directors. Traditional exchanges cannot achieve openness and transparency of assets, and the main reason is that they are subject to technical constraints, and the birth of blockchain technology makes this goal technically feasible. The mission of Liberum Decentralized Exchange is to convert such feasibility into real practice. Relying on the blockchain technology and the concept of the token economy, Liberum Decentralized Exchange will establish a real-time asset and transaction data query verification mechanism and make it publicly available.

The transaction system of Liberum Decentralized Exchange can realize the financial-level fastness and stability, making all transactions efficient and secure. Liberum Decentralized Exchange provides the security-level advanced algorithm, supporting GTT, GTC, FOK, IOC and many other professional transaction orders, so as to offer users professional quantitative support.

Liberum Decentralized Exchange is committed to providing global users with value flows and user experiences, building the most transparent, shared and democratic ecological transactions for users, creating the world's most influential innovative autonomous decentralized digital asset transaction platform, solving the liquidity problem of digital assets, optimizing the allocation of social financial capital, improving the efficiency of asset allocation, and solving the financing needs of projects with industrial advantages. Meanwhile, it will provide a safe, fair and open transaction platform for global digital technology fans.

4.4.2 Basic Function Module

(1) Market Quotation

The market quotation module is mainly to collect, analyze and investigate the related information of market quotation, for the purpose of providing users with accurate, efficient and professional information about digital currencies.

(2) Transactions between Digital Currencies

The module of transactions between digital currencies is mainly for realizing the fast, highly frequent and low-cost transactions between different digital currencies.

(3) Digital Currency Asset Management

The asset management module is mainly for managing all user assets (including digital currencies and legal tenders), and can show the quantity, unit price, equivalent legal tender value and other related information of digital currency assets owned by users in a real time manner.

(4) Digital Asset Mall

In the digital asset mall, users can directly use their digital currencies to buy goods and services. The platform will pay the merchants in legal tenders after automatic conversion according to the market price.

4.5 Subchain Project

Currently, multiple projects and applications are being tested on the Liberum public chain. Typical applications based on subchain include:

4.5.1 Decentralized anonymous chat software (in beta)

Liberum decentralized anonymous chat software is a subchain based on Liberumunderlying system but using proof of stake consensus. Combined with the most concise and efficient decentralized instant messaging protocol DIM Protocol on the market, it has developed a communication layer to better achieve a completely decentralized blockchain social full ecological chain network service. It aims to achieve free communication, encrypted communication, secure transactions, distribution according to work, and interconnection of upstream and downstream industries in a digital asset society, and to provide global digital world enthusiasts with all-eco social communication (including cross-chain and cross-platform instant messaging), content sharing, project airdrops, cross-border payments, and market conditions interpretation, real-time information, blockchain e-commerce, games, entertainment, peer-to-peer advertising, and digital asset exchange. At the same time, by introducing third-party content and service providers and DIM network participants via the IM open platform, it shares and expands the global ecology of the currency circle and chain, and activates the flow of trillion-scale digital assets, so that every user who joins the Liberum decentralized anonymous chat software family may enjoy fast, efficient and secure services in the most cost-effective way.

4.5.2 Decentralized anonymous Q&A software (in beta)

Decentralized anonymous Q&A software is a fully decentralized application based on Liberum subchain. It is currently developed by Liberum enthusiasts. Users can get information by asking questions and get rewards by answering questions.

Liberum decentralized anonymous Q&A software will handle Q&A and distribution of benefits. These logics are recorded on a Liberum subchain through a smart contract. For such applications, there is no need for any back-end database or development of blockchain. The entire business logic can be completed based on the platform token.

LIBERUM

Chapter V

Economical Model of Liberum

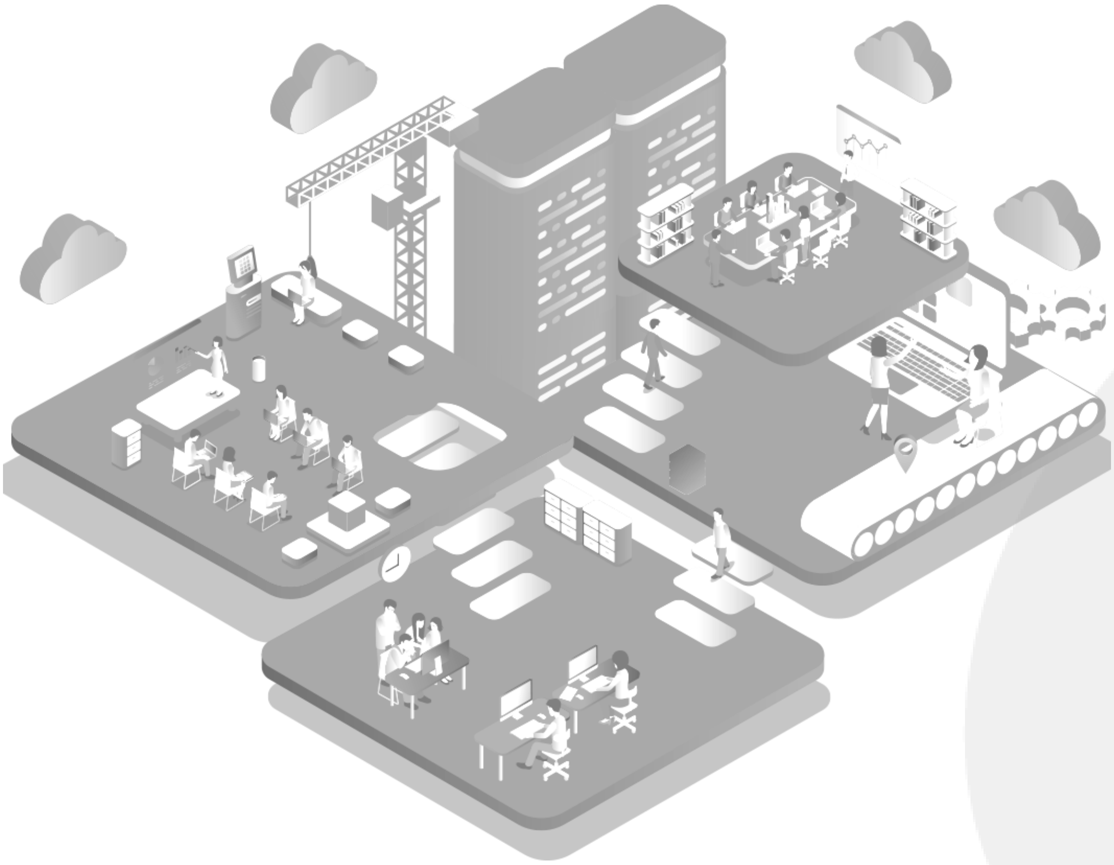
Chapter V. Economical Model of Laber

5.1 Introduction to Laber

Laber (hereinafter referred to as "LBR") is the built-in and protogenetic encrypted digital token of LBR network, which can be used in transaction, settlement and smart contract performance on the chain. LBR can conveniently represent and measure the digitized economic activities in LBR. Its value is based on the following two points. Firstly, a certain amount of LBR token will be consumed as the fuel by the applications on the LBR chain. Secondly, LBR token holders can participate in the governance of LBR blockchain communities.

As the key link to maintain the operation of LBR ecosystem, LBR token guarantees the successful establishment of the ecosphere closed-cycle, and functions to circulate value, buy services, get returns and encourage interaction. It can be applied in many scenarios within Liberum and under the Liberum Ecosystem, and will be applied in all ecological chain projects on the Liberum platform in the future.

LBR will positively inspire community members such as platforms, miners and users and help Liberum to achieve ecological health. At the same time, it provides a safe, fair and open transaction platform for digital currency enthusiasts, and controls the black-box operation method through transaction platform technology and monitoring measures, so as to ensure fair transaction of digital money lovers around the world.



5.2 Issuance and Initial Distribution of LBR Public Blockchain

5.2.1 Attribute of LBR Public Blockchain

- Size of issue: 980 million tokens
- Issue price: 0.2 dollar
- Block interval time: About 10 seconds
- Output of single block: 72 LBR (432 LBR /minute, 25,920 LBR /hour, 622,080 LBR /day, 227.0592 million LBR /year)

5.2.2 Mining Mechanism of LBR

- In the first 12 years, reduced by half every two years

First time (1st - 2nd year): 454,118,400 tokens

Second time (3rd - 4th year): 227,059,200 tokens

Third time (5th - 6th year): 113,529,600 tokens

Fourth time (7th - 8th year): 56,764,800 tokens

Fifth time: (9th - 10th year): 28,382,400 tokens

Sixth time (11st - 12nd year): 14,191,200 tokens

- In the second 12 years

85,954,400 tokens will be mined out in 12 years on average, with 7,162,866.66 tokens every year.

5.2.3 Realization of LBR values

(1) Transaction fee

Laber can be used to pay transaction fees for transfers, node creation, consensus joining, consensus withdrawal, node cancellation and aliase setting on the Liberum network.

(2) **Smart contract consumption**

The creation, invocation, transfer and deletion of smart contracts all require Laber.

(3) Consumption of chain-building

Users may conveniently create their own chains by using Liberum’s chain factory chain-building service. The use of chain-building services requires the consumption of LBR.

(4) Circulation and consumption of cross-chain assets

Through Liberum’s module warehouse service and chain factory chain-building service, a Liberum-based chain ecology can be created. There are multiple independent chains in this ecology. They can make cross-chain transfers through the Liberum main network, and their respective digital currencies can be transferred on this ecological chain.

If these chains want to support cross-chain transfers, register will be needed; at this time, they need to lock the corresponding Laber for cross-chain consumption. If the locked Laber is consumed to the minimum, it needs to be replenished, otherwise cross-chain transfers will be impossible.

(5) As voting rights

The governance of community can be achieved by exercising the right to vote.

5.3 Decentralized Self-governed Community

The core functions of Liberum are developed by its global decentralized team. The core team members are mainly responsible for the development and maintenance of main chain, and do not interfere with development or operation; other ecosystems are freely developed and operated by the technology volunteers, code contributors, etc. It is an epitome of real decentralized consensus society in the charge of nobody and everybody at the same time, which is fully open-source and self-governed by depending on consensus. It is a free consensus society based on all people.

We have added a decentralized voting consensus self-governing system in Liberum, so as to ensure the ecology will also develop in a sound way according to the consensus of all participants when the development team ofLiberum quits its guiding role.

Liberum does not belong to any individual or organization; instead, it belongs to all humans hoping to be anonymous. The decentralized freedom, consensus and self-governing is a great subversive practice. When most blockchain projects are still under the control of centralization, the stock voting mechanism of Liberum has ensured the ecology to develop according to the wills of all people. Based on the decentralized force, Liberum brings the world back to an environment full of love, respect, freedom and equality. In this more perfect world, everyone will embrace real freedom and permanence.

Chapter VI

Implementation Route

Chapter VI. Implementation Route

In August 2017, a decentralized financial promotion group was established;

In October 2017, the direction of the decentralized all-ecological future currency network plan was formulated;

In November 2017, the product concept and logic were initially constructed;

In January 2018, the underlying architecture was developed;

In August 2018, product features were upgraded;

In January 2019, the underlying architecture of technical framework was completed;

In June 2019, the decentralized consensus society's ecological future currency network plan was confirmed;

In July 2019, the project was officially named Liberum;

In October 2019, Liberum development was completed and final testing was performed;

In December 2019, the program and itsWhite Paper will be officially released;

In January 2020, Liberum will be launched.

Disclaimer

In this article, all technologies are now in the R&D and testing stages and they will be affected by future changes, improvements and innovations. Although the Liberum decentralized financial promotion team takes security very seriously, the platform may still have loopholes, so there is no guarantee that the process of creating and processing cryptocurrencies on the platform will not be disturbed or error-free. In addition, the software may contain inherent risks, such as defects, weaknesses, vulnerabilities, viruses, or errors.

In addition, all cryptocurrencies carry risks associated with acquiring storage transfers and using digital currencies, and the Liberum public chain faces the same risks. It is warned that Liberum supporters should carefully read the relevant instructions contained in this White Paper, fully understand the blockchain, recognize the potential risks, and fully evaluate their risk tolerance and actual conditions for rational judgments.

Reference

[1]S.Nakamoto:"Bitcoin:A peer-to-peer electronic cash system” ,2008.

[2]V.Buterin,Ethereum:"A Next-Generation Smart Contract and Decentralized Application Platform” ,2014

[3]Paul Sztorc: “Market empiricism” .

[4]Casey Detrio: “Smart markets for smart contracts",2015.

[5]Goldman Sachs:Blockchain-Putting Theory into Practice

[6]Shafi Goldwasser,Silvio Micali and Charles Rackoff:” The Knowledge Complexity of Interactive Proof-Systems” .

[7]Nick Szabo:"Smart Contracts:Building Blocks for Digital Markets” ,1996

[8]Hal Finney"Reusable Proofs of Work",2005

[9]Peter Thiel:"From Zero To One”

[10] “Advertisement,Is it necessary in the digital age?” (SERI Research essay)/Samsung Economic Research Institute

[11]"Digital Media and Advertising” Hanul Academy

[12]Park,Kikyoung: “Customer Response to Customer Satisfaction Survey Participation” ,2015

[13]Amrit Tiwana: “"Platform Ecosystems:Aligning Architecture,Governance,andStrategy” ,2018

[14]Nicholas Gregory Mankiw “Principles of Economics”

[15]Christian,Catalini,Joshua,S,Gans.(2016) “Some Simple Economics of the Blockchain” Rotman School of Management,Working Paper No.2874598;MIT Sloan Research Paper No.5191-16

[16]Sinclair,Davidson,Primavera,De,Filippi.,Jason,Potts.(2016) “Economics of Blockchain” paper presented to Public Choice,US,March 2016.

[17]ICON Hyperconnect the World [Internet].[last updated 31 Jan 2018].Available:https://icon.foundation/

[18]Steem-An incentivized,blockchain-based,public content platform [Internet].[cited

aug 2017].Available:https://steem.io/

[19]https://github.com/theloopkr/Loopchain/blob/master/README_KR.md

[20]Forbes Online Magazine(www.forbes.com)article titled “Cyber-crime costs projected to reach $2 Trillion by 2019” ,Steve Morgan(Jan 17,2016).

[21]Markets and Markets research analyst report(www.marketsandmarkets.com) titled “Cybersecurity Market by Solution,Service,Security Type,Deployment Mode, Organization Size,Vertical,and Region-Global Forecast to 2022” (July,2017).

[22]Published pricing data from CASB providers Skyhigh Networks,Bitglass and Cloudskope.

[23] “Sia:Simple Decentralized Storage” ,David Vorick and Luke Champine(Nov 29,2014).

[24] “Filecoin:A Decentralized Storage Network” ,Protocol Labs(Aug 14,2017).

[25]Published access latency data from Sia,Filecoin,Ethereum,Bitcoin,Litecoin, Ripple,Hyperledger,Maidsafe,Google,Rackspace and Amazon.

[26] “A Tutorial on RAID storage systems” ,Sameshan Perumal and Pieter Kritzinger

(May 6,2004).278. “Ethereum White Paper:A Next Generation Smart Contract and Decentralized Application Program” ,Vitalik Buderin(January,2014).

[27]Hyperledger Project,www.hyperledger.org,Open source development project managed by the Linux Foundation,(December,2015)

[28] “BigchainDB:A Scalable Decentralized Database” ,Trent McConaghy,Rudolph Marques,Andreas Muller,Dimitri De Jonghe,Troy McConaghy,Greg McMullen, Ryan Henderson,Sylvian Bellemare and Alberto Granzotto,(February,2016)

[29]Spencer Gimball,(February 2014):Cockroach DB design document,github.com/ cockroachdb/cockroach/blob/master/docs/design.md

[30]Leemon Baird:"The Swirlds Hashgraph Consensus Algorithm:Fair,Fast,Byzantine Fault Tolerance” ,(May 31,2016).

[31] “Bitcoin-Statistics and Facts” ,Statistica,www.statista.com/topics/2308/bitcoin/ (October 2016).