THE KAICOIN WHITE PAPER

“ KAICOIN, Which is the Cryptocurrency Platform

Changing The Value of Currency ”

www.kaicoin.io

Initial Ver. 1.0: May 1, 2017

Last Updated Ver. 1.2: August 18, 2017

CONTENTS

1. Summary

The KAICOIN is invested and developed by KAii to increase the profit of KAii members and to use the payment of the worldwide contents concerning KAii.

The KAICOIN is developed to supplement the technical skills of Bitcoin and Ethereum and developed to enhance the transmission speed by 10 times and to keep perfect security.

Especially KAICOIN is estimated as security – centered cryptocurrency.

The total supply of the KAICOIN is confined to 2.1 billion and the KAICOIN brings the value-rising effect according to the scarcity of itself in spreading over the World.

In addition, the surrounding system has been already built to use mobile-games, e-shopping malls, and VR contents and so on.

Afterward the surroundings to use will be fast extended.

The KAii itself will operate the consolidated exchange system.

This means to pursue the profit of the members through the perfect security system and to enter into dealing with KAICOIN, Bitcoin, Ethereum, and the several noted Alt-coins.

2. Background

The blockchain was implemented as the central technology of Bitcoin in 2009 by Satoshi Nakamoto. Bitcoin used blockchain to solve the double spending problem, which is the main ground for as a financial transaction ledger where individuals Publicly record transfers of currency.

Afterward there have been numerous Altcoins leveraging blockchain technology.

There are about eight-hundred cryptocurrencies, which are competing and trading successfully throughout the world.

Today many of companies and banks are investing for technology of

cryptocurrency through consortium blockchain.

Blockchain technology are researched and developed by several groups concerning with digital assets besides currency transaction, financial, products, services, logistics information, property, identity, and so on.

Following Bitcoin, Ethereum was developed on July in 2014 by Vitalik Buterin.

Ethereum has its blockchain providing smart contracts which can be used to create contracts that can be used to encode arbitrary state transaction functions.

The aim of the blockchain based on smart contracts is to allow users to write any kind of contract(or program) onto the blockchain and the smart contracts can be used to developed : decentralized marketplaces and currency exchange platforms.

However, there are some problems with Bitcoin.

One of the problems is delayed transmission speed. (payment/remittance)

Another is narrowness of the block volume. In the Ethereum case, the problem is security vulnerability(the problem of DAO program).

Today the concern for the 4th currency, Cryptocurrency, is rapidly spreading all over the world.

Accordingly the more secure and convenient coin is requested now.

KAICOIN complements the negatives of Bitcoin and Ethereum. It has been developed to increase convenience and profitability by concentrating on block chain technology, which is focused on e-commerce based on Korean culture.

3. About GSChain

GSChain is a platform customized for creating and distributing specific block chains between organizations. GSChain aims to solve the problem perceived as a barrier to the circulation of block-chain technology in the financial sector by giving privacy

and guidelines through a simple package. Derived from the Bitcoin Core software, GSChain supports Windows, Linux, and Mac servers, and supports a simple API and command line interface. In the following section, we will introduce the first public release of GSChain and its features.

3-1. Private block chain

GSChain provides a solution to problems related to mining, privacy, and openness by unifying the management of user authority. The main objectives of GSChain are summarized as follows.

1) Block chain activity is visible only to selected participants.
2) Introduce a control method for which transactions are allowed.
3) It can be mined safely without any related expenses such as proof of work (PoW).

If the block chain is privatized, the problem of expanding the block can easily be solved as the block chain participants can simply change the maximum size of the block. Furthermore, as it is a closed system, only transactions related to certain participants occur.

All passwords begin with the use of public key cryptography to manage identity and security. Cryptographic users randomly generate their private keys and never disclose them to other participants. Each private key has a mathematically linked public address, which replaces an identity that can receive funds. Once the funds are transferred to the public address, the private key is required to "sign" the transaction. This means that accessing the private key holds the funds protected by that particular key. This cryptography controls access to the funds and enables users to sign messages to verify that they own the private key associated with that

particular address. Because of this feature, GSChain allows only the users included in the access list to access the block chain. When two block chain nodes are connected, they are "verified" as follows.

These cryptosystems control access to funds, and the user owns the private key associated with a particular address.

1) Each node identifies its public address on the access permission list.
2) Each node checks whether the other party's address exists in each allowable list.
3) Each node sends a challenge message to the other party.
4) Each node sends a signature of the received challenge message to prove that it has a private key corresponding to the existing public address.

The principle of linking authority to a public address can also be applied to the other functions of the network. For example, you can restrict the transfer and/or receipt transaction privilege to a specific list as both the sender and recipient addresses are detailed in the transaction history. As there are multiple settlements and/or recipients, the transaction will only be allowed if the sender and the recipient included in the transaction are on the "allowable" list. Browsing the block chain publicly and limiting the transactional abilities can also be performed. Finally, you can limit the mining in GSChain by adding a signature column to the coin-based transactions that miners have included in the block. This plays an important role in preventing a small number of people from mastering the private block chain, which is mentioned in the following section.

GSChain authority

In GSChain, all authorizations and cancellations are conducted by using network transactions that contain specific metadata. The "genesis" block miner has all access rights including the administration rights to manage other users' rights. The

administrator grants privileges to other users through the metadata that stipulates the user address contained in the transaction output value and the privileges to be approved to each user. Further restrictions apply when modifying the administrative and mining rights of other users. Existing administrators must vote on whether they accept the changes, and a minimum percentage must be met to change the rights. These votes are recorded by each manager in a separate transaction, and the changes are reflected when a consensus is met. At the beginning of the block chain generation, a few blocks constitute a "setup phase," where one administrator can skip the aforementioned voting. In future versions, GSChain may reflect a "super administrator" that can independently grant or revoke authorization.

As the modifications are embedded in the transactional metadata, they circulate quickly to all the nodes in the network, which results to an agreement on the current state. However, as it is a distributed network, each node may receive authorization transactions at different times either before and/or after other transactions.

If the payment transaction validity is determined to be a change of authority that has not yet been circulated, this difference can be fatal—some nodes may accept payment and some may decline the payment. This difference is resolved when a transaction is identified in the block chain, and the final order is fixed. As a transaction is "played" in the order of block chains, each transaction in the block must be a valid transaction based on the previous user's authority. If the transaction in the block is invalid, the entire block is annulled. Even if the block is valid, it must be validated in the "allowed" list defined in the transaction of that block.

However, access rights are excluded from this authorization management system as they are not related to the contents of the block chain. As an alternative, when

the privilege of a specific address is rescinded, all nodes disconnect from the node that used the address during the "response verification" process. For convenience purposes, it is also possible to grant temporary rights to block numbers in a fixed range. A transaction based on this temporary privilege is valid only for block numbers in the specified range. The change of authority is considered to be consensual only when a sufficient number of administrators have correctly designated the appropriate block range for the user and authority. This increases the transparency of the network and reduces the load of having to cancel temporarily expired privileges individually.

For the block chain to be accurately "private" networks, all addresses are accepted in chains, and at least one administrator must know the actual identity of the recipient. However, most participants do not need to know each other's identity. One of the main functions of a block chain is peer-to-peer (P2P) transactions, in which two types of tokens are exchanged. If the anonymity of the address is guaranteed, transactions can be made without knowing the real identity of the other person as the transaction progresses. Even though financial institutions handle multiple addresses and transactions, only the person in charge can know the real owner of each address.

3-2. Mining in GSChain

GSChain provides the mining rights only to the parties who can identify certain people, resolving the dilemma of a private block chain where one person can monopolize the mining right/s. This solution is possible by limiting the number of blocks that the same miner can generate within a certain period. There are certain parameters required when implementing these constraints.

Mining diversity (Defined as: 0 ≤ mining diversity ≤ 1)

Validating blocks with parameters

1) Apply all the privilege changes defined in the transaction in the block consecutively.

2) Count the number of licensed miners after the change is applied.

3) Multiply the miner by the mining diversity, and round off the result to get the spacing value.

4) If the miner of the block has mined the last spacing-1 block, the block is annulled.

In this schedule, which is formatted like a round-robin, the licensed miners rotate once to create a block, which is a valid block chain. The mining diversity parameter is defined by a strict schema scheme, which refers to the percentage of licensed miners that must be bumped to secure the network. A value of 1 means that all licensed miners are included in the cycle, and a value of 0 means that there are no restrictions. In general, a larger value is considered a secure network, but if it is too close to 1, some of the miners may be jammed in that block chain when they are inactive. Therefore, a median value of 0.75 is recommended. Each node will try not to be mined in the last spacing-1 block that it has already mined to conserve resources.

Constraints on diversity variables can prevent malicious activities and can help when the network is temporarily disconnected due to a disruption in communication. During this time, a division in a block chain may occur as a node of a broken network section cannot see a transaction or a block of another section. After the network is restored, a universal consensus is made based on the longest fork in the chain. This diversity constraint ensures that the longest block chain belongs to the zone with multiple permissible miners. During this time, the block chain of another section will also be frozen.

Usability of private block chains

There can be questions raised on why a private block chain is used rather than a centralized database. Centralized databases can also accept incoming transactions, resolve conflicts, and respond to database status queries. There are three answers to this question, as follows.

1) In a block chain, each participant controls his or her assets completely via a private key. Miners cannot create transactions with another participants' funds.
2) As the database control is distributed among numerous participants, it is not possible for a specific person or a smaller group to judge the existence of a transaction alone.
3) A block chain is more stable than the centralized database system. If a server goes missing or fails, it will not affect transactions across the whole network.

What about PoW for rights-based mining? To ensure mining diversity, Bitcoin makes computational work required for mining through the PoW problematic (i.e., expensive). On the other hand, a private block chain guarantees mining diversity through a much simpler method, so the work required for the PoW is only perfunctory. As a matter of fact, the first version of GSChain still uses a Bitcoin-style PoW to regulate and randomize the block production rate of each node, but the same cannot be said for a device for securing the block chain.

In a GSChain block chain, transaction commission and block compensation are set to 0. If the block mining cost is tiny, the miners do not need to compensate separately. It will be mined for the benefit of the smooth functioning of the block chain. Instead, miners may obtain a fixed annual fee for network participants, paying by means of payments in the scheme rather than in a block chain. If the goal of the block chain is to provide transactions to be tokenized assets, then the

encryption of the network in question can be ignored. However, if a transactional shortage is desired, GSChain can be configured to use cryptography as a means of block compensation, minimum transaction fee, and transaction volume. In this case, the participant must purchase the encryption money from the miners, and the means of purchase may be tokenized assets.

3-3. Multiple block chain drives

Instead of supporting a single block chain like the Bitcoin Core model, it is easy to configure and operate several block chains at the same time in GSChain. At an institutional level, it is highly advantageous that system administrators, not specific developers, can construct and operate a private block chain. It is simple to create and use a database with several SQL commands in a relational database management system (RDBMS) such as an Oracle or SQL server. Furthermore, the advantage of supporting multiple block chains is that the server can connect activities into different chains. For example, if funds come into a certain block chain, they can be sent to another one.

All parameters of the block chain that can be set by the user in GSChain are listed in the following table.

1. Chain protocol	Make it similar to a private block chain or Bitcoin Core.
2. Target time per block	1 min, etc.
3. Authorization type	Anyone can connect or receive some.
4. Mining diversity	e.g., 0.75
5. The level of consensus required to create/remove managers and miners, and the duration of the setup phase where this is not enforced	Private block chain only
6. Mining compensation	e.g., 50 units per block; set to reduce by half every 210,000 blocks

7. IP port and JSON-RPC API required for P2P connections	e.g., 8571, 8570
8. Transaction types allowed	e.g., Pay-to-address, pay-to-multisig, pay-to-script-hash
9. Maximum block size	e.g., 1 MB
10. Maximum metadata per transaction	e.g., 4,096 B

You can activate multiple block chains on a server, and each block chain has its own name and configuration file. To create a new block chain, the user must make two settings.

1) The user selects the chain name. GSChain will then create a configuration file with the default settings. This file can then be modified by the user, and the default settings are usually enough to carry out this task.

2) If the user runs a block chain, GSChain will scrap the first block and give the creator all user rights. Now, the details of the initial block and the parameter hash of the corresponding block chain are embedded in the configuration file to prepare for future mistakes.

GSChain process

When performed for the first time, the block chain operates as a single node. To add a node, GSChain executes with three parameters on another computer.

(1) Destination block chain name

(2) IP port number

(3) IP address of the existing node

For convenience purposes, this information is in the form of "node address."

For example, gschain@127.0.0.1: 0000. As it is a private network, the new node cannot connect to the network without access permission. GSChain will display a

message that contains the publicly generated address of the new node, which must be sent to the administrator. The administrator then creates a connection with a simple command and grants access to that address.

The new node will then be able to connect and automatically download the configuration file that defines the characteristics of the block chain when connected. Later on, when reconnecting to the same block chain, only the chain name is required, and the verification procedure authenticates that both nodes are using the same parameters.

GSChain improvements

One of the things that must be improved in the future is to allow some parameters to be changed through certain connections issued by trusted administrators when the block chain is up and running. For example, as the volume of network usage increases, the maximum block size to inherit the transaction volume must also be increased. For this change to occur, one must consider the computing power of each node on the network.

3-4. Multi-currency block chain

Block chain – It was mentioned before that using a tokenization protocol, such as CoinSpark or Counterparty, can issue and trade third-party assets in a Bitcoin block chain equivalent to Bitcoin's own currency. This technique can be used in a private block chain generated by GSChain without any modification. However, block chains that use private protocols can be upgraded further by incorporating the ability to support third-party assets into chain rules.

In Bitcoin, the number of Bitcoins embedded in each transaction result value is encoded for each transaction. If there are more Bitcoins in the input value than in

the output value, the corresponding transaction is invalidated in the network and neither checked nor propagated to the block chain. This verification is possible as every node in the network tracks the Bitcoin in the exhausted output value. Therefore, users can be rest assured that the amount of Bitcoins inherent in the transaction content will be correct through the transaction itself in the network or block chain. This allows a "simple payment verification" wallet to trade securely with the network, eliminating the need to store an entire block chain on the user's computer.

Tokenization issues

The problem with tokenizing an asset in a Bitcoin is that the metadata that encodes the external asset does not go through a network-level verification process that verifies the Bitcoin itself. For example, suppose a bank ("ABC") issued a token that symbolized the dollar. A malicious user can create a transaction with metadata that the output value is 100 ABC dollars. However, the transaction did not have an ABC dollar in the input. These transactions are validated in the Bitcoin network and are also verified in the block chain as the Bitcoin nodes cannot read this metadata and does not track the ABC dollars.

Thus, the tokenized asset is subject to a second public treatment comparative to the Bitcoin currency in the Bitcoin block chain. The presence of a tokenized asset can be determined by looking at all transactions that affect the token since the transaction in which the token was originally created. This can efficiently be calculated in a "forward" manner. Every time a new transaction comes in, it is mandatory to have it reviewed. However, even then, a whole network node is needed, and the tokenization protocol is not suitable for use with insubstantial wallets.

To solve this problem, GSChain encodes the identifiers and quantities of all assets in each transaction output value. During this specific time, the extension provided by the Bitcoin script language is used. This allows the transaction validation rule to be extended to verify that the total amount of all assets in the transaction output value is exactly the same as that in the input value. The requirement that the input and output values must be the same is more stringent than the requirements of the Bitcoin itself. In the case of Bitcoin, if the output value is less than the input value, it is processed without any problem. At this time, the differencing amount goes to the mining fee. Before using this approach, you must allow the block chain to create new assets through the first transaction through the use of special metadata. GSChain automatically assigns an identifier for a new asset based on where the initial transaction is generated on the block chain and is used with a unique identifier defined by the user.

The authorization system of GSChain may be used to control asset creation rights. Future versions will also have the ability to introduce rights by asset, which will allow administrators and allowed senders/recipients to be set up on a per-asset basis. It is a feature not included in the initial version of GSChain because of simplicity issues, but it can be added easily by a simple extension to already-reflected rules.

3-5. Switching between Bitcoin and a private block chain

When Internet usage boomed in the 1990s, millions of people were exposed to a new paradigm. Companies wanted to use these novelties internally, but at that juncture in time, companies did not have adequate privacy, reliability, and capacity to use the Internet as a primary mode of communication. Therefore, many companies created "Intranet," which internalized the Internet. It used the same

infrastructure and technology as the Internet, but it was technology that was completely controllable by the company.

Fast forward 20 years and now the Internet has become a network capable of delivering large amounts of information consistently and dependently across the globe. This has led many companies to use virtual private networks (VPNs). VPN utilizes the Internet as a basic technology but encrypts the communication contents of the organization and can maintain security even when broadcasted through a public communication network. This makes it possible to enjoy the uses of the Internet without having to expose it to the outside world.

Similar procedures are in progress for Bitcoin block chains and private block chains. From the perspective of a merchant, the Bitcoin network has not been under control yet. This is because Bitcoin's capacity is limited, and its long-term transaction costs cannot be projected. Most importantly, however, Bitcoin mining is mostly controlled by an undetermined number of people, most of whom are in countries with conflicting philosophies or unestablished legal systems. Thus, for financial institutions, the use of these technologies in the next decade will be a more attractive and lucrative option. In 20 years' time (just like the 20-year Internet boom), if Bitcoin and/or other block chains are managing billions of transactions each month at a very low and sustainable cost, and large corporations are controlling their mining efficiently, then Bitcoin can be a very attractive platform for financial institution transactions. By adding a thin encryption layer like VPN, the activities of the organization can be hidden from most network participants.

The GSChain concept design aims to make switching between a private block chain and a Bitcoin block body in many ways possible. If you have an application that uses asset tokenization and messaging via the five features mentioned as follows,

you can switch between Bitcoin and private block chains with little to no code changes.

1) GSChain is based on a derivative version of Bitcoin Core, the official client of the Bitcoin network. Code changes are localized and can accompany Bitcoin improvements in the future.
2) GSChain uses a platform similar to that of Bitcoin's protocol, transaction, and block chain architecture. The only difference is the response verification procedure that occurs when both nodes connect for the very first time. The rest of the functions are altered by modifying the legitimacy rules of metadata and transactions/blocks.
3) The GSChain interface (command line, API) is fully compatible with the Bitcoin Core interface. Additional functionalities were also included with some new commands.
4) GSChain can act as a node in a generic Bitcoin network (or a Bitcoin-like network) with a simple protocol setting in the per–block chain configuration file.
5) The multi-currency and messaging functions of GSChain works are very much like the CoinSpark protocol to improve Bitcoin transaction.

4. KAICOIN application technology

4-1. Block chain method

To prevent preoccupancy and monopoly from a particular group or organization, starting clearly with the information about pre-mining and restoration to the society, true or not. Everyone can join the mining, the KAICOIN shares compensation with public blockchain method.
Accordingly, the security of the cryptocurrency system in question is higher up.

Public blockchain is called permissionless Ledger. This means that anyone else can read and verify the blockchain data without permission.
The KAICOIN follows this tech skill and anyone can download the blockchain, inquire any data and participate the record by signing code.
Participants can decide input a certain data, or not by voting. There is a common way for giving voting rights in proportion to the computing power that is inserted, and not to the relative amount of nodes. However, in this method, KAICOIN does not allow nodes with a strong computing power to be monopolized via mining diversity. Thus, a large amount of nodes are used to possibly succeed in mining.

4-2. Block time and block size

From the beginning, the KAICOIN has its 3,000~4,000 members, so the speed of transaction and the security is very important.
Thus by making the block size from 4 kbyte to 2048 kbyte and the speed of transmission enhance, the steady speed of transmission can be obtained.
We can chain hashing block in 60 seconds by fixing 60- second blocktime. You can (it is possible to) experience the advanced hash technique of advanced SHA256, which is 10 times faster than the 10 minute block time of the existing bitcoin.
These two issues can block off miscarrying and delaying payment system, and so ensure security itself as Bitcoin.
By choosing the 2048 kbyte which is thought to be the most effective blocksize, we can settle the former blocksize problem.

4-3. Multiple signature script

Pay to Script Hash(P2SH) can provide the coding that is required two signature simultaneously to be used easily. P2SH can alternate the coded.
Hash Power with digital letters by using the complicated script, and P2SH can

provide the effective system of transmission systematically including Merit of reducing the volume of transaction.

4-4. Half-life

It provides an open mining system that can be mined for a total of 100 years based on one half-life year. It can be estimated that about 1,576,800 blocks will be formed in a total of three years based on 1-min block time. This is to ensure a better mining environment for the miners. Taking into consideration the initial issue volume of 2.1 billion, it is not possible to progressively allot the ecosystem of the block chain responsible for security. If mining opportunity, difficulty, and sufficient periods are provided, then this is a possibility.

Creating a mining environment with a slightly better working environment is authentically fulfilling the original purpose of the block chain technology.

4-5. KAICOIN specifications

- Hash algorithm: Advanced SHA256
- Total volume: 2.1 billion KAICOINs
- Issuing method: Mining
- Block time: 60 s
- Block size: 2,048 kB

5. About KAICOIN

5-1. Purpose

The KAICOIN is developed by overwhelming desire of KAii members who are wanting to improve the out-of-date system of cryptocurrency. The KAICOIN is the cryptocurrency that meets the needs of users such as security, speed, and transparency.

The issuance way of KAICOIN is mining and its Hash Algorithm is SAH256 Script, which can supplement the shortcomings of Bitcoin such as the delayed transmission speed and the security vulnerability.

Above all, the blockchain of the KAICOIN is developed to focus on e-commercial. This means that the users of the KAICOIN can use the coin more conveniently and economically.

The KAICOIN must be the medium of payment of 10,000 subsidiary companies of the KAii and each company will build the systematic and cooperative network. The KAICOIN has its goal to be the best global cryptocurrency which can be used as e-commercial coin across the world.

This is creating a block chain system that can be used in various ways in everyday life. It will contribute to the development of society and culture by merging Korea's distinctive contents and culture. Through this, KAICOIN will be universally recognized as a virtual current that is commonly used internationally.

5-2. Application platform

Today due to the fast development of ICT (Information and Communications Technology), no one can survive the competition with old-fashioned method (thoughts and minds).

To meet the requirement of the age, the platform-basement appeared and it's

been positioned as a key factor to success or failure of the companies.

The platform-based cryptocurrency (Ethereum) is developed at first by Vitalic Buterin in 2014. Unlike Bitcoin which has function as simple money, Ethereum is different From Bitcoin in conception.

From now on, the platform-based cryptocurrency like Ethereum will lead the age of the 4th Industrial Revolution and make general trend. The KAICOIN is also the platform-based cryptocurrency and via the KAICOIN, the KAii will develop various activities in the realm of business and social donation.

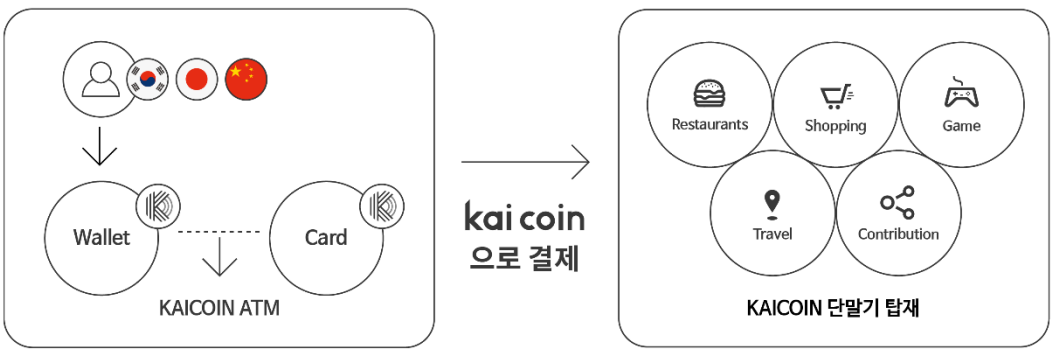
Social	- Expansion of social structure through the sharing of block chain technology - Support of nonprofit activities by establishing a social input platform and the transparent financial support of NGOs
Culture	- Completion of a marketing platform in China and Japan through K-Culture–based contents - Expansion of VR content and mobile video navigation using a distributed system - Securing off-line merchants such as restaurants, bakeries, travel agencies, and hospitals - Expansion of domestic/overseas online shopping mall support - Online game internal item trading support
Economy	- Establishment of KAICOIN Integrated Exchange (KAIREX) - Utilization of KAICOIN as an automatic teller machine (ATM) - KAICOIN listed on the International Exchange

5-3. Additional information

- Coin name: KAICOIN
- Coin units: KAI
- Preselling period: (GMT+9) September 1, 2017, 12: 00 p.m.
  to October 31, 2017, 11:59 p.m.
- Price per token: 1,500 KAI = 1 ETH
- Minimum purchasing amount: 150 KAI = 0.1 ETH
- Total supply: 200,000,000
- Trading currency: ETH
- Bonus: State discrimination payment
  (~20% for Week 1, 15% for Week 2, 10% for Week 3, 5% for Week 4, 0% for Week 5)

Total supply 2,100,000,000	Open mining volume	1,000,000,000
	Amount of line mined	**1,100,000,000**
Amount of line mined 1,100,000,000	Pre-sales in Korea	600,000,000
	ICO	**200,000,000**
	Social contribution	100,000,000
	Investor holdings	100,000,000
	Miscellaneous	100,000,000

5-4. Service environment



5-4-1. Game

Items mean a variety of instruments on the on-line games and items are traded like a spot among game-users. Beside of game items; "game-money" and "accounts" are subject to trading of course.

On starting a spot-site treating cash – business of items; the bigger derivatives market more than the on-line game industry begins eventually.

Therefore the game-development company concentrates on developing items of derivatives prior to game-development and the success or not of games depends on the game-price in question.

KAICOIN will be used as a term for gaming money (currency) using certain games, and there will be a lot of demand in domestic and overseas markets.

5.4.2. Online shopping mall

On-line shopping is said to surf and order the goods by using the internet, the personal computers, and the mobile phones. Payment is done by the credit cards and the mobile-pays.

This on-line shopping show rapidly increasing tendency according to growing information communication technology and growing the users of the internet and spreading convenience. But on-line shopping has several problems: personal information extrusion, unstable payment system.

And so the cryptocurrency is developed into the new payment means.

On this, the KAICOIN can solve the problems of the instability of payment system, the double spending problem, exposing identity of the payers, and excessive charge in paying.

KAICOIN will solve the problems of the existing payment system such as double payment problems, payer identity exposure, and excessive commission problems.

5.4.3. On-off line merchants

Franchise is a shop or a store which is belonged to a business union.

Franchising is a kind of contract between a shop and a business union. Franchise can expect to get creating profit and managing assistance through brand name from the business union.

Nowadays the number of franchise is increasing explosively. The KAICOIN will cooperate with the companies holding famous brand and try to be the KAICOIN as the means of payment.

5-4-4. Mobile service

- KAICOIN Wallet : An electronic purse that allows you to manage your account by receiving a cash coin
- KAIREX : Exchange services to trade KAICOIN and other virtual currencies
- Donations/miscellaneous : Search for domestic and overseas KAICOIN merchants, various gifts and donations, and possible donation services

6. Road map

1st phase (–September 2017)	- KAICOIN development - Charter agreement with KAICOIN - ICO Korea Pre-Sale completed - Launching of ICO Global Pre-Sale - Launching of KAICOIN Wallet
2nd phase (October–December 2017)	- Launching of KAICOIN Exchange (KAIREX) - Getting listed on the International Exchange list - Expansion of partnership with vendors and PG companies

3rd phase (2018)	- Combination of the use of KAICOIN and card - Easy payment made by ATM and coins - Use of KAICOIN in everyday life
4th phase (2019)	- Supporting of billing system in China and Japan - Securing of more than 10,000 off-line merchants - Expansion of support centering on the travel industry - Offering of special convenience for Chinese and Japanese tourists
5th phase (2020–)	- Seeking to enter Southeast Asian and European markets - In both domestic and overseas markets, making KAICOIN highly utilized in real life and a monetary policy representative

7. Developers and affiliates

The KAICOIN was founded on December in 2010. The KAii is nonprofit organization and its goal is to assist the economic education, the investment education and the angel investment club and to campaign the stock-contribution through cooperation with lots of partners, and to bring up about hundred –thousand sound investors.

The business of the KAii is categorized into four parts.

First, Financial Education Business

This business gives the members the asset management and investment education and economic education service to the youth through the financial education program of the KAii Academy.

Second, Promotion Business for Investment Club

This business gives the members the investment opportunity by finding valuable companies throughout the angel-club foundation and the operation assistance.

Third, Stock-Sharing Business

This business means the cooperating network business with 7,000 subordinate companies. As a part of social communities, the KAii is willing to join the innovative stock-sharing compaign and to practice the social responsibility.

Last, Digital Industry Investment and its Operating Business Based on Information Technology. The KAii founded the Headquarter of KAICOIN under the KAii, considering the new cryptocurrency which is required to the Fourth Industrial Revolution and the payment system, in particular security, speed, and profit.

The KAICOIN will be used by not only the KAii and its members but also the partners. And the KAICOIN will be used as the global game companies and on-line shopping malls, and the franchises with famous brands.

Due to the characteristics of the cryptocurrency, the value of the coin will be up in increasing the supply compared with the limited total coin amount, which will provide the profit with members holding the KAICOIN.

7-2. Affiliates

KAii	WHITE STONE	Allreve	INCAPO
WOWZONE	PICK:LE JAPAN	PICK:LE CHINA	AllStarWORLD
Rosenbee Medical	Bulgogi restaurant	Tuna restaurant	Kangnamnamu hospital

※ Affiliates without homepages will be excluded.

※ You can get more information about new affiliates on the homepage.

- KAii: http://www.kaii.or.kr/default/mindex.php
- Allreve: http://www.allreve.com/mshop/main.asp

- WOWZONE: http://wowzone.co.kr/mshop/main.asp
- PICK:LE Japan: http://ameblo.jp/pickle-japan
- PICK:LE China: http://weibo.com/u/5888766483?is_hot=1
- AllStarWORLD: http://www.allstarworld.co.kr
- RosenBee Medical: http://www.rosenbee.com
- Kangnamnamu Hospital: http://www.knamu.co.kr/index.asp

8. Conclusion

The KAICOIN Headquarter which is the branch company of the KAii has strived for only developing an advanced cryptocurrency and exploiting the Value of Bitcoin and the platform basement of Ethereum.

This technology has been developed specifically to specialize in game and e-commercial payment. The KAICOIN Development Team has built a block chain–based system that can be used in various ways in everyday life by utilizing the security and morality that can be attained through the block chain technology. It will contribute to the development of society and culture by combining Korean contents and culture. This move will lead to an internationally accepted virtual currency.