



# HyperChain

Blockchain infrastructure

For Everyone

## **Abstract**

This document uses Proof of Activity (POA) to verify events caused by actions and introduces blockchains based on them. POA is used in the HyperChain ecosystem to calculate the contribution of operation generated by the actions of participants and to distribute reasonable rewards. Blockchain networks participating in HyperChain network configuration can all be expressed within HyperChain by configuring appropriate interfaces. This means that an independent blockchain network can evolve by configuring its own protocol in addition to the Connect Protocol and modifying it on its own.

In other words, HyperChain's goal is to build an easy-to-use infrastructure for the popularization of Blockchain. This will bridge the gap between the cryptocurrency market and consumers, removing barriers to access, bringing it into the mainstream by helping the general public trust and understand what we believe is the future of Blockchain.

The contents below assume that we basically know about general Blockchain protocols and encryption such as Bitcoin.

# Contents

|   |    |
|---|----|
| <b>Important Notice</b> .....                 | 4  |
| <b>Introduction</b> .....                     | 6  |
| <b>Current History</b> .....                  | 6  |
| <b>Principle</b> .....                        | 7  |
| <b>Glossary</b> .....                         | 8  |
| <b>Feature</b> .....                          | 11 |
| <b>Network Design</b> .....                   | 12 |
| <b>Proof Of Activity</b> .....                | 12 |
| <b>Account Storage</b> .....                  | 13 |
| <b>Helix - Pyramid</b> .....                  | 14 |
| <b>Instant Token System</b> .....             | 15 |
| <b>Double Spent Protection</b> .....          | 15 |
| <b>Operation Hash</b> .....                   | 16 |
| <b>Blockchain Network Configuration</b> ..... | 17 |
| <b>Block</b> .....                            | 19 |
| <b>Cryptographic Integrity</b> .....          | 19 |
| <b>Important Notes</b> .....                  | 20 |

# Important Notice

HyperChain's digital coins (hereinafter referred to as "SNC") are not intended to constitute securities, units of collective investment schemes, or other capital market instruments as defined in accordance with the Securities and Futures Act (Cap. 289).

SNC does not grant you any ownership or other interest in the teams, companies, etc. related to the HyperChain project.

Nothing in this whitepaper should be treated or understood as a guarantee or promise as to how HyperChain's business or SNC will develop or the usefulness or value of the Coins. This white paper outlines the current plan that can be changed depending on the situation. All statements regarding future events are based on the HyperChain project team's analysis of the issues described in this white paper. That analysis may turn out to be erroneous.

The HyperChain Economy may not materialize, or if it fails, it may not be possible to recover the amount paid for the SNC.

The content of this white paper is not intended to be a sales proposal or purchase recommendation by SNC.

This white paper is provided to provide information about HyperChain's SNC Economy and features, and to receive feedback and opinions.

According to this white paper, no one is obligated to enter into any contract or binding legal undertaking in relation to the sale or purchase of SNC.

This White Paper or any part of this White Paper may not be taken or transmitted to any country where distribution is prohibited or restricted.

The contents of this white paper cannot be conveyed without including "Important Notes".

In case of unauthorized use or distribution in relation to this white paper, civil and criminal actions may be taken in accordance with relevant laws.

We recommend that you use this white paper only for reference purposes to plan and vision.

# Introduction

The well-known Blockchain is an implementation of a fault-tolerant replication state machine. Currently, each of these publicly known Blockchains has limitations for various reasons. HyperChain is a Blockchain that is solving the limitations of these existing BlockChains. HyperChain's main focus is solving the "scalability problem". Various Blockchain projects are adding a lot of additional content as well as the initial project goals. As a result, it is becoming a Blockchain that is progressing differently from what was initially intended, and even the phenomenon of the Blockchain project being terminated. HyperChain provides and supports the Connect Protocol that connects Blockchain networks to overcome the limitations of Blockchain's expansion and develops its own protocol with its own content. For the smooth agreement of these Blockchain networks, Proof Of Activity (POA) was presented, and POA is designed to define sequence and type and create ledger in Operation according to action (in HyperChain, it is called Operation under the concept of expandable transaction). All networks participating in HyperChain are expected to be able to proceed depending on the order of operation of the wallet recorded in the ledger.

## Current History

On August 15, 2018, the HyperChain Team published a white paper describing Proof Of Activity, a technology that validates and trusts behavior. Each action has a sequence number as a nOperation, and it can be determined in the order of the sequence number to see who takes precedence, so computers that do not trust each other simplify mutual synchronization. As a result of this simple synchronization, the network can be very fast, limited only by the network bandwidth.

When HyperChain was released as TestNet Ver.0 in 2018, it was confirmed that other blockchain projects at the time were struggling to process more than 15-30 transactions per second. Therefore, in HyperChain TestNet Ver.0, many tests were performed through communities, social media (SNS), online markets, etc. as an initial POA (Proof Of Activity) mechanism. With the

participation of various users, we proceeded to enable more stable and faster processing such as 1 second of Block Time and instant transaction.

With this development progress, HyperChain released MainNet Ver1.0, a stable version of TestNet, on June 15, 2020, and started a full-scale HyperChain project.

HyperChain Ver1.0 applies the Instant Token System to solve the token code and security problems of fragmented DAPP by easily composing the token ecosystem by anyone, and strengthening the security by applying the block of the Helix-Pyramid structure. In addition, a multi-layered architecture was introduced to speed up processing and facilitate participation.

On July 5, 2021, HyperChain Ver2.0 was released with a stable version of a multi-layered architecture and an independent blockchain network and interconnection. The main feature of HyperChain Ver2.0 is that a blockchain with mutually independent networks connects one or more networks to perform mutual verification. With the release of HyperChain Ver2.0, anyone can quickly proceed with the block chain constituting the main network, and the goal of HyperChain, "Everyone Can Enjoy," has been partially realized.

For more stable processing, HyperChain Dev Team went through numerous discussions and released a dramatically improved version of HyperChain Ver3.0 on January 1, 2022 regarding the verification and processing of nOperation. Super Network, Speed Network, and Smart Network (3S), the core of the Triple Core applied to Ver3.0, implements a sharing economy ecosystem in which users grow together according to HyperChain's slogan.

## Principle

HyperChain 3.0 Triple Core has three principles to construct an easily accessible infrastructure for the popularization of Blockchain.

- Everyone can enjoy

Users do not need a deep understanding of various concepts such as public and private blockchains. We dream of popularizing blockchain by building an infrastructure that anyone can easily access and realize their ideas to their heart's content.

- Let's grow together

This principle is inspired by the concept of the sharing economy. The principle of the sharing economy refers to economic activities recognizing the fact that goods are leased and used with each other rather than owned. Platform businesses based on such a sharing economy are being serviced in various forms, and HyperChain also wants to build a blockchain ecosystem where all users become owners of the platform and share the profits generated. In other words, the HyperChain is the MainNet that connects the blockchain with an independent network.

- Fast-Easy-High Security

The chain must guarantee a minimum block creation time of 1 second, instant transaction completion, process a minimum of 5,000 TPS, and not incur high transaction fees that exceed the required cost. In addition, transaction fees must be stable. HyperChain provides stronger security in the form of a multi-chain (1-4-3) rather than a simple block connection based on the Helix-Pyramid structure, and the processing speed of 30,000 cases has been tested. It is evolving to theoretically handle more than 100,000 cases.

## Glossary

The following terms are used throughout the document.

- Hash  
A digital fingerprint of a sequence of bytes.
- dApp  
Decentralized application.
- HN  
HyperChain Network.
- BN  
BlockChain Network



- **Bootnode**  
Bootnodes that helps HNs and BNs to register themselves in the network and to discover other nodes to connect to.
- **SNC**  
SNC is the main internal transferable cryptocurrency of HyperChain and is used to pay transaction fees when creating or executing operations or when transferring SNC.
- **Block reward**  
Newly issued SNC and the sum of transaction fees used in the block.
- **HMC**  
HyperChain Mined Coin
- **BMC**  
BlockChain Mined Coin
- **Operation**  
A transaction container that plays a role similar to that of an existing blockchain. A transaction that can do more than just value on the HyperChain Network..
- **Account**  
A record in the HyperChain ledger that either holds data or is an executable program. Addressable by a key, often referred to as a public key or pubkey.  
  
The key may be one of:
  - secp256k1
  - secp384r1
  - sect283k1
  - secp521r1
- **Account Owner**  
The address of the program that owns the account. Only the owning program is capable of modifying the account.
- **Block**  
It is a set of contiguous entries in the ledger. It has a 1-4-3 structure.

- Blockhash  
A unique value hash that identifies a record block.
- Block height  
The number of blocks beneath the current block.
- Genesis block  
The 0 ~ 4 block in the chain.
- Keypair  
A public key and corresponding private key for accessing an account.
- Private key  
The private key of a keypair.
- Public key(pubkey)  
The public key of a keypair.
- Signature  
A signature of R and S. Each operation must have at least one signature.
- Token  
Assets made with Instant Token System.
- Coin  
A minable crypto currency registered when an independent network is formed.
- Wallet  
A collection of keypairs that allows users to manage their funds.

# Feature

- **High Speed and Low Costs**  
It is transmitted immediately without delay and does not charge high costs for transmission.
- **Fair Deals Only**  
HyperChain supports fair and transparent transactions between each blockchain.
- **Protection From Attack**  
On a blockchain platform, every user account is independent. It is protected from attack.
- **Cost Effective**  
Scale economy through decentralization leading to significant decrease in transaction fees.
- **Blockchain Connection**  
Participating block chains can be interlinked and can be used as a single platform.
- **Easy Entry and Fair Competition**  
It is easy to participate in Blockchain and operate the network, and through the selection and support of users participating in the HyperChain Network, the Blockchain Networks can compete fairly.
- **Various Platforms**  
It can be used equally on multiple platforms with a single account system and operation system.
- **Real-Time Operation**  
Operations created in the connected chain are verified and processed in real time through PoA (Proof Of Activity) and Helix-Pyramid.

# Network Design

The network constituting the HyperChain Connect Protocol is composed of the Chain Network constituting the system and the Blockchain Network that has an independent protocol. In the Chain Network, according to the amount of activity, the system leader is designated and ready to record blocks, and in the rest of the network, the generated operations are verified and provided as a leader network. Operations that have reached the leader network and have been verified can be efficiently processed by other networks by allocating the sequence number (opblock) of the operation to be recorded in the block. Run Operation in the current state stored in RAM and propagate the final state to another Chain Network. Check the final state in the chain network, and propagate to the entire network.

- When the chain is not split, there is one system leader on the network at the same time. Nodes constituting each Chain Network have at least the specified minimum hardware specifications and can be elected as system leaders. Election of system leaders is carried out through POS based on staking and POA based elections according to the amount of network activity when participating in Chain Network.

## Proof Of Activity

Proof Of Activity is a method to designate the order of Events (Operations) occurring in the Account and to check the amount of activity. In order to create an operation in the account you have, you need to know the number of operations that have been created in the account so far at the time the operation is created.

In other words, by adding a value of 1 to the value of  $n_{Operation}$ , which means the sequence number of Account, to the operation creation requirement, it must match the sequence number of the operation to be created to create an operation. In other words, it is possible to determine whether the operation created in the account is normally created before signature verification, and the order of the user's actions is guaranteed sequentially.

In addition, when the operation created by the Account is recorded, the activity activity of the Account can be judged by recording/updating the PassiveBlock (Operation receiving block) and ActiveBlock (Operation sending block) of the Account. In addition, each operation calculates an activity point called an Action Point or Stemina Point, and based on this, the amount of activity

in the Account is calculated more precisely.

## Account Storage

Account Storage is designed to operate as follows.

For Example:

| Acc. Index | Pub Key | Balance | C Block | nOperation | passBlock | actBlock |
|------------|---------|---------|---------|------------|-----------|----------|
| 10         | PubKey  | 9       | 10      | 2          | 104       | 7        |
| 11         | PubKey  | 0       | 18      | 0          | 18        | 18       |
| 12         | PubKey  | 105     | 22      | 1          | 2100      | 70       |
| 13         | PubKey  | 90000   | 70      | 1          | 80        | 250      |
| 14         | PubKey  | 700     | 2100    | 8          | 2105      | 3333     |
| ...        | ...     | ...     | ...     | ...        | ...       | ...      |
| n-1        | PubKey  | n-1     | n-1     | n-1        | n-1       | n-1      |
| n          | PubKey  | n       | n       | n          | n         | n        |

Account Storage is structurally composed of Account Segments. Each Account is divided into Index and PublicKey, and consists of the balance, the block number for which the account is activated, the number of operations created, the block that has received the latest operation, and the block that created the most recent operation. Account Storage adds a New Account Segment when Account Active Operation is created and Confirm proceeds in Block.

Account storage managed in this way will play an important role in the Proof Of Activity described above. The operation created in each account is executed based on the index and public key, and it is used for quick operation processing and spam prevention. Some examples are as follows.

- When creating an operation in Account, the value of nOperation is included in the Operation object and created. By comparing the value of nOperation included in Operation with nOperation recorded in Account Storage, the creation of real-time spam using multiple nodes is restricted. By using it as a pre-processing process for verification of the generated operation, it is possible to filter the verification of meaningless operation.

- In addition, the order can be guaranteed by sequentially aligning the actions of the account based on the value of nOperation. This makes it easier to verify the signature performed in the process of verifying and processing the operation.
- Existing blockchains have a very difficult point in checking the history of the account with the blockchain system itself. Based on the contents recorded in Account Storage, it is possible to determine when the account was activated, what is the block number that received the operation, and how many operations were created in addition to the block number that sent the operation. History can be quickly checked. This means that unlike the existing Blockchain, which requires many additional elements for the Blockchain system, the Blockchain system itself can be maintained and sustained.

## **Helix - Pyramid**

Helix-Pyramid, represented by HyperChain, has three multi-connection structures, unlike the one-connection structure method of other existing blockchains..

The connection structure here refers to a structure in which blocks are connected by pointers using hash, etc., and has the characteristic of being connected to the three blocks of the previous order according to the chain mechanism that connects.

At this time, the connected chain has a multi-chain form called Helix-Pyramid. This means that HyperChain's block structure is not a simple block connection, but several blocks are connected and managed.

When Block Commit is in progress, -1, -4, and -3 hashes are verified and a caching hash is generated. This can be configured as a PAM (Point Access Method), and the configured PAM is a point used to verify the POA (Proof Of Activity) in the leader network according to HyperChain's Network Design and to determine the preferred preference of the block. This point is used to give the sequence number of operations occurring in HyperChain Network and works for fair processing of only large amounts of operations occurring in a particular Network Node or Account. This Helix-Pyramid structure is the main mechanism of HyperChain, and you can check the tech doc for more details on this part.

# Instant Token System

HyperChain's Instant Token System is a system introduced in v1.0, and was introduced according to the needs of users, such as fees and production conditions, which are used for creating tokens through the existing ERC20 and using only basic functions such as transmission. Basically, the Token System consists of Normal and Advance. In the case of Normal, only Token's transmission and storage functions are supported, and in the case of Advance, Token System provides preferential support for functions with needs, such as changes to Token System's owner, lock-up, time lock-up, incineration, and additional issuance. The Instant Token System is a system that is mainly used before configuring an independent Blockchain that basically constitutes HyperChain or when only the basic functions of Token are required.

## Double Spent Protection

One of the most important elements that make up and use Blockchain is the Cryptocurrency transfer part. The part where double spending can occur when transferring Cryptocurrency is a potential part of various blockchains.

In HyperChain, it is also used in POA (Proof Of Activity) and solves the double-spending problem through nOperation, which plays an important role in the network.

Hash of operation created in HyperChain Network (similar to txhash in other blockchains) has an order for each operation for POA processing. This order is a part called nOperation, has elements of nOperation for each account, and is used as Incremental Value for the order of activities. This is because the operation created in each account must have a value of  $nOperation + 1$ , so it is impossible to process more than one operation with the same nOperation value for the operations created in the account. This part works as a double-spending prevention.

Since this nOperation is important in HyperChain Network, it is important to understand and use it correctly.

# Operation Hash

The hashes of operations created in HyperChain Network are configured to include the nOperation mentioned above. The Operation Hash created by the account allows you to know the order of activity in the account.

Operation Hash It consists of 32 bytes and contains the following information.

- 4 bytes are composed of Block Number of Chain. A value of 0 in this part means that there is no information about the block number on which this operation was executed. In other words, if the value is 0, it means that there is no information about the block or it has not been processed as it has been included in the network's mempool (pending operation).
- 4 bytes are composed of the Index Number of the Account that created the Operation. (In case of Multi Operation or Multi Sender, it means the final signer.)
- 4 bytes are composed of the value of nOperation of the previously recorded Account Index Number.
- The remaining 20 bytes are composed of Hash like md160 for Operation Info.

12 bytes excluding hash, which consists of 20 bytes, are each composed of a little endian and mean a hexadecimal value. When an operation is processed, both the operation hash with block information and the operation hash without block information are correct and treated equally.



# BlockChain Network Configuration

BlockChains who want to participate in HyperChain Network have to go through several steps. In HyperChain, this is called nine steps. Each node that proceeds with the configuration can be achieved on its own or with the support of users participating in the HyperChain Network, and is complementary..

Nine Steps consists of the following.

1. Register master node.

In order to register and operate a node, you need to register the wallet address of the master node to participate in.

Register your wallet address, prove your possession of SNC, and proceed with lockup. If the requirements are met, you will be given an authorization code for the Network..

2. Master node hardware verification

The hardware that constitutes the master node of the BlockChain Network is inspected and approved if the requirements are met..

3. Super node configuration

Master nodes that have succeeded in all of the preceding procedures must recruit or configure five super nodes to be configured together. Super node also registers wallet address and proves holding of SNC, and as it is configured, it notifies master node of its intention to participate. The master node can approve or reject the super node by receiving the super node's intention to participate, and when there are more than 5 approved super nodes, the configuration process is performed primarily.

4. Super Node Hardware Verification

Hardware verification of the previously requested super nodes is required, and each super node must meet the hardware specifications required by each BlockChain Network, and requests hardware verification from the master node. This also requires confirmation and approval of the master node as described above.

## 5. Standard Node Configuration

The master node and super node must configure the standard node to be configured in the super node. The standard node must consist of 100 standard nodes for each super node.

A standard node does not require hardware verification and consists of a proof of ownership of the SNC and a request for participation by a super node. Super nodes can approve or reject standard nodes that have requested participation.

## 6. Coin Info registration

Once all nodes to participate with the master node are registered, you must register Coin information to be configured on the Blockchain Network. The registration contents include the method and distribution rate.

## 7. Node Test

Before actually operating the nodes of the configured Blockchain Network, verification of each hardware that will operate the master and super nodes, and tests such as blocks, transactions, and mining are conducted. The duration of the test can be configured from a minimum of 7 days to a maximum of 30 days.

## 8. Test Verification

Nodes that have been tested are subject to verification process. If the verification is successful, the actual node operation can start, and mining is also possible.

## 9. Node Platform Play

Blockchain Network is constituted, and actual operation of Nodes is started based on the progress, and Blockchain Network for an independent purpose is configured and proceeded.

# Block

Blocks are created independently of each other in HN (HyperChain Network) and BN (Blockchain Network), SNC in HyperChain Network and Coins set in each network in Blockchain Network are mined. In the HyperChain Network Protocol, as described above, it follows the rules of the HyperChain Network, and in the Blockchain Network, it proceeds according to the rules of the Blockchain. In general, when the master node of Blockchain is started, notification is made on characteristics such as Coin along with the goal of Blockchain Network. In other words, the independent Blockchain Network has an independent block recording system and enables the operation of an independent platform.

## Cryptographic Integrity

Blockchain Networks, which constitute HyperChain Networks, will be carried out by sharing the Crypto Current system in addition to the platform suitable for each Blockchain system. The factor that makes this possible is the account storage described above. Account Storage plays an important role in preserving the cryptographic integrity of the entire Blockchain, because Account Storage organizes and contains the actions of actions created by the block. The BlockHeader of HyperChain Network is processed by including the Hash of Account Storage.

# Important Notes

- **Disclaimer of liability**

To the maximum extent permitted by the applicable laws, regulations and rules, HyperChain Team shall not be liable for any indirect, special, incidental, consequential or other losses of any kind, in tort, contract or otherwise (including but not limited to loss of revenue, income or profits, and loss of use or data), arising out of or in connection with any acceptance of or reliance on this Whitepaper or any part thereof by you.

- **No representations and warranties**

HyperChain Team does not make or purport to make, and hereby disclaims, any representation, warranty or undertaking in any form whatsoever to any entity or person, including any representation, warranty or undertaking in relation to the truth, accuracy and completeness of any of the information set out in this Whitepaper.

- **Representations and warranties by you**

By accessing and/or accepting possession of any information in this Whitepaper or such part thereof (as the case may be), you represent and warrant to HyperChain Team as follows :

- You agree and acknowledge that SNC does not constitute securities, units of collective investment schemes, or other capital market instruments or equivalent instruments respectively defined under the SFA or other regulated instruments of any jurisdiction..
- You agree and acknowledge that this White Paper does not constitute a prospectus or offer document and is not intended to constitute an offer of securities, units of a collective investment scheme or other capital market instruments, respectively, as defined in accordance with the SFA.  
Recommendation or solicitation of any equivalent or other regulated product or investment in any jurisdiction, and you are not obligated to enter into any contract or binding legal commitment, and you shall not accept digital tokens

or any other payment method on the basis of this white paper.

- You agree and acknowledge that SNC will not be construed, classified or treated as providing any recipient or buyer an opportunity to participate or receive any profit, income, or other payment or return arising out of or in connection with HyperChain.
- You acknowledge that no regulatory authority has investigated or approved the information set forth in this white paper and has not or will not take any action pursuant to any law, regulatory requirement or rule regarding the publication, distribution or dissemination of this white paper. dissemination of this Whitepaper to you does not imply that the applicable laws, regulatory requirements or rules have been complied with;
- Distribution or dissemination of this white paper, part or copy, or your acceptance of it is not prohibited or restricted by applicable laws, regulations, or rules in your jurisdiction, and where any restrictions related to ownership apply, you shall comply with all such restrictions at your own expense.
- You have a basic understanding of cryptocurrency, blockchain-based software systems, blockchain technology, and smart contract technology's operation, functionality, use, storage, transmission mechanisms, and other material characteristics.
- You fully recognize and understand that there are risks related to cryptocurrency exchange and its business and operation when you want to purchase SNC.
- In addition, HyperChain Team is not responsible for updating future forecast statements or publicly announcing amendments to future forecast statements to reflect future developments, events, or situations, even if new information is provided or other events occur in the future..
- Please note that this Whitepaper is also only a work in progress and the information in this Whitepaper is current only as of the date on the cover hereof. HyperChain Team reserves the right to update the Whitepaper from time to time.

- **Restrictions on distribution and dissemination**

The distribution or dissemination of this Whitepaper or any part thereof may be prohibited or restricted by the laws, regulatory requirements and rules of any jurisdiction. In the case where any restriction applies, you are to inform yourself about, and to observe, any restrictions which are applicable to your possession of this Whitepaper or such part thereof (as the case may be) at your own expense and without liability to HyperChain Team. Persons who have been provided access to this Whitepaper or to whom a copy of this Whitepaper has been distributed or disseminated or who otherwise have the Whitepaper in their possession shall not circulate it to any other persons, reproduce or otherwise distribute this Whitepaper or any information contained herein for any purpose whatsoever nor permit or cause the same to occur. If the contents of this white paper are used for commercial purposes without permission, or illegally collected, reproduced, distributed, etc., civil and criminal actions may be taken in accordance with relevant laws.

- **Risks and uncertainties**

The responsibility for the consequences of making decisions using this white paper lies entirely with the party who made the judgment, and the team shall not bear any responsibility for damages, losses, debts, or other damages incurred in relation(Regardless of profit or loss) to the use of this white paper.

- We recommend that you use this white paper only for understanding and rough reference purposes of the vision and future plans pursued by Team.
- HyperChain described in this white paper is the mainnet that connects independent blockchains, and the blockchain participating in HyperChain has its own regulations.
- HyperChain's coin described in this paper is a coin with price volatility and has nothing to do with legal regulations such as legal currency, currency, and stocks other than cryptocurrency (virtual currency).
- This white paper cannot be construed as legal, financial, or accounting advice under any circumstances. In the process of purchasing and using SNC, separate laws, finance, accounting, taxation, etc. may occur in accordance with policies and laws of each country and region.