

# **HyperCube: A New Smart Contract Platform With Energy Efficiency**

HyperCube: A New Smart Contract Platform With Energy Efficiency .....	1
Declaration of Free Blockchain .....	5
Abstract.....	5
Introduction .....	5
Overview .....	5
Positioning of HyperCube? .....	6
What is XPZ?.....	6
Origin of HyperCube .....	7
How Hypercube Makes Money .....	8
Latest Information.....	8
Working Partners .....	8
<b>Architecture.....</b>	<b>11</b>
Proof of Dedication.....	13
Existing Problems for Blockchain Consensus Algorithm .....	13
Necessity to Expand the Ethereum .....	14
D-Value.....	15
Node Selection .....	16
Factors of D-Value.....	16
Network .....	18
Protocol Overview.....	18
<b>MINO</b> Records.....	<b>18</b>
MINO Interface.....	18
<b>PUSH MESSAGE</b> .....	<b>18</b>
<b>PUSH PEERS, PRUNE MESSAGE</b> .....	<b>18</b>
<b>PULL MESSAGE</b> .....	<b>19</b>
<b>PURGING</b> .....	<b>19</b>
Tokenomics .....	20
Terminology .....	21
Current Supply Cap.....	21
Inflation Index.....	21
Supply Time Table.....	21

Viable Inflation Index .....	22
Staking Yield [%].....	22
Token Dilution [%].....	23
Adjusted Staking Yield [%] .....	23
Supply Time Table .....	24
Tailored Staking Yield .....	27
Token Dilution .....	27
Mining.....	30
Hardware Specification .....	30
Mining Colleterial .....	31
Mining Processing Pipeline.....	32
TxCreator .....	33
TxSigner .....	33
TxSyncor.....	34
HyperPool .....	34
Constructing a HyperPool.....	34
Becoming a member of a HyperPool.....	35
Transacting with a HyperPool.....	35
Transaction Confirmation.....	35
Alpha Node .....	36
Rotation .....	37
Alpha Node Schedule Rotation with Epoch Sized Partitions.....	38
Alpha Node Schedule Generation at Genesis .....	38
Schedule Attack Vectors.....	39
Appending Entries .....	40
Miners Sync .....	40
POD and VDF .....	41
Storage.....	43
Blockthread .....	43
Persistence .....	43
Repair.....	43
Forks .....	44

Restart .....	44
Build .....	45
XVM Virtual Machine .....	46
XRC20 Standard .....	47
XRC77 Standard .....	47
XRC155 Standard .....	48
Standard Mass Transfers .....	48
Multiple Token Contracts .....	48
Integrated Token Type Detection.....	48
Secure Token Transfer .....	49
XRexx .....	49
Introduction of XRexx .....	49
Robust Analysis of XRexx.....	51
Metaverse .....	55
HyperVerse .....	55
MetaPlant.....	59
DApp Link.....	59
NFT Browser/Market .....	59
Collaboration Platform .....	59
Network Traffic Entrance .....	60
NFT Extension.....	60
DApp Link .....	61
Social DApp .....	61
Conclusion .....	62
Reference .....	62

# Declaration of Free Blockchain

## Abstract

This article offers a novel blockchain architecture based on Proof of Dedication (PoD) - a proof for determining the prominence and authenticity of nodes at multiple dimensions, such as uptime, capacity, and commitment service time. PoD is a data structure that is used to encrypt the safe transit of events into a ledger. It is an append only data structure. POD is a hybrid of Proof of Work and Proof of Stake that can lower message cost in a Byzantine Fault Tolerant replicated state machine, leading in sub-second finality times.

This article also offers two protocols that take use of the PoD ledger's event-keeping properties: Evernet, a permanent data infrastructure for storing persistent data, and Blockthread, the equivalent data structure.

We presented a way to be compatible with already established networks, such as Ethereum. We think this approach is valuable because it lays the groundwork for future implementations capable of attaining global-commerce levels of scale and anonymity.

## Introduction

### Overview

HyperCube was established in August 2017 to build a better blockchain and intelligent trading platform. The HyperCube network is being built to enhance global banking and payment systems. HyperCube is the first digital currency designed for enterprises. Since Bitcoin, HyperCube is the first novel Satoshi Nakamoto consensus method that includes BFT.

It was developed by researchers in HyperCube Labs and is called the Proof of Dedication. The team includes top engineers from Google, Netflix and Amazon, as well as distinguished scholars from Stanford University, Cambridge University and Oxford University, as well as IEEE standard setters. XZP Virtual and the new intelligent transaction programming language XRexx from HyperCube are powerful, auditable and secure. Atomic swaps, authorized payees, recoverable wallets, multi-signature wallets, and rate-limited wallets are examples of smart transactions that are currently accessible.

## Positioning of HyperCube?

In the second half of 2021, POW mining public chains such as BTC and ETH will enter a new round of bull market. At that time, PoW and other conceptual sectors will have new attention and hot spots. At the same time, the characteristics of slow PoW and high gas fees will also be prominently displayed. The new HyperCube public chain will launch a new PoD mining formula algorithm.

The POD algorithm is based on HyperCube's self-developed network dynamic equilibrium formula, combined with the BFT algorithm, to locate network records in multiple dimensions from energy, time, online time, and community investment. Account privileges can obtain higher network security than EThash (the consensus algorithm of cryptocurrency on Ethereum) while maintaining high speed. The HyperCube public chain is a two-layer expansion solution compatible with Ethereum, which can expand the landing of Ethereum. With the existing powerful ecology of Ethereum, HyperCube will become a powerful part of Ethereum in the future, challenging Ethereum's current dominant position in the smart contract platform.

HyperCube was born for financial and social applications. HyperCube is a set of officially launched Ethereum layer 2 expansion solutions. It is a side chain network that applies the PoD consensus protocol, allowing highly scalable games and user-oriented DApps to run on top of it, while still being affected by Ethereum. The security support of the workshop.

## What is XPZ?

XPZ is the native token of HyperCube. The total amount of XPZ is 2.1 billion.

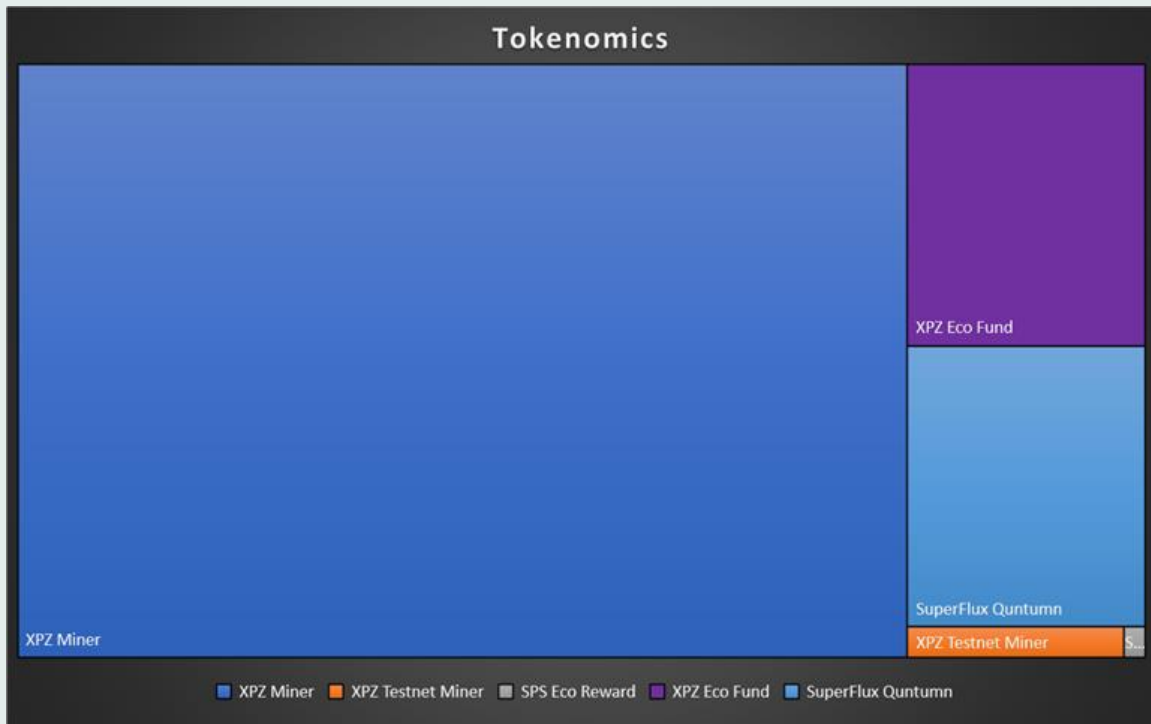


FIGURE 1 TOKEN DISTRIBUTION

## Origin of HyperCube

Since we first introduced the basic concept of HyperCube in 2017, the core team at HyperCube Lab has been working on finding a solution to have a decentralized node network function on par with a single node for the past four years. This is a characteristic that no other major blockchain is capable of matching. The achievement of this aim is the ultimate goal of HyperCube.

Since its inception, the HyperCube team, which is comprised of pioneering technical experts from organizations such as the IEEE, Amazon, Netflix, Intel, Netscape, and Google, has been concentrating on the technology required to build HyperCube in order to meet these ground-breaking performance specifications.

The transaction processing speed of proof-of-work-based systems like Bitcoin and Ethereum is approximately ten times faster than that of traditional systems (TPS). Tendermint and other practical Byzantine Fault Tolerance (PBFT)-based Proof of Stake (PoS) systems support 1,000 TPS for 100–200 nodes, and other PBFT-based systems support 2,000 TPS for 100–200 nodes. With more than 50,000 transactions per second (TPS) and more than 100 nodes in its current testnet iteration, the PBFT-like proof-of-work blockchain HyperCube is the world's fastest blockchain and the world's first network-scale decentralized network.

## **How Hypercube Makes Money**

HyperCube positions itself as a free and open source platform where anyone can access its products, including technologies, products and services.

## **Latest Information**

[HyperCube Github Repo](#)

[HyperCube Official Telegram](#)

## **Working Partners**

As a result, the HyperCube team independently developed the world's first cross-chain traceability and anti-counterfeiting system based on blockchain technology with a multi-industry and multi-chain architecture, and is committed to creating information transparency, collaboration efficiency, and value using the blockchain trusted network architecture. High-speed transmission of multi-chain traceability value information ecological environment. The project team comes from industry elites in many regions of the world. After long-term efforts, the current basic application model has achieved the standards for massive adoption.

## **University of Cambridge**

The University of Cambridge was founded in 1209 and is located in Cambridge, England. It is one of the top universities in the UK and in the world. Many famous British scientists, writers, and politicians come from this university. Cambridge University is also the institution of higher learning with the largest number of Nobel Prize winners. About 80 Nobel Prize winners have taught or studied here, and more than 70 are students of Cambridge University. The University of Cambridge is also a member of the "Russell Group", an alliance of prestigious universities in the United Kingdom, a member of the Coimbra Group, an alliance of universities in Europe, and one of the British Golden Triangle Universities. The University of Cambridge and the University of Oxford are the two best universities in the UK, collectively known as "Oxbridge", and are one of the top ten universities in the world.

## **Oxford university**

Oxford University in the United Kingdom has a worldwide reputation. It has an extremely important position in the British society and higher education system and has a worldwide influence. Many young students in the UK and around the world have set their ideals for further studies at Oxford University. The University of Oxford is a British research university Russell Union, the Coimbra Group of top European universities, and the European Research University Alliance. For nine



centuries, Oxford University has been a top university in the UK and even in the world. Oxford University and Cambridge University are often collectively called Niu Jian, and they are the oldest and most famous universities in England. From 2002 to 2013, Oxford University has been ranked as the top university in the UK by The Times for many consecutive years.

### **Imperial College**

Imperial College London (Imperial College London), also known as Imperial College London, or Imperial College for short, was established in 1907 and is located in London, England. It is a member of the Russell University Group, one of the BRIC schools, and a member of the European IDEA Alliance. The world-renowned top universities in the world ranked second in the 2014/15QS World University Rankings. Imperial College London, Cambridge University, Oxford University, London School of Economics, and University College London are collectively known as the "G5 Super Elite University". Its research level is recognized as one of the top three universities in the UK and is famous for engineering, medical, and business studies. . The British education community has a reputation for "three pillars". The liberal arts are Oxford, the sciences are Cambridge, and the engineering is undoubtedly the Imperial College.

### **IEEE**

IEEE (Insititute of Electrical and Electronics Engineers) is the world's largest and most important non-profit professional society leading the development of electronic and electrical technology in the world. IEEE was formed in 1963 by the merger of the American Society of Electronic Engineers (founded in 1884) and the American Society of Radio Engineers (founded in 1912). At the beginning of its establishment, IEEE has established the following main work directions:

### **Grayscale Investments**

Grayscale Investment Company is registered in the United States, the world's leading blockchain investment institution. Grayscale Investment Co., Ltd. manages more than 10 billion U.S. dollars of encrypted assets, and its investment scope covers more than 100 countries in the Americas, Asia, and Europe.

### **Coinbase Ventures**

Coinbase Ventures has always been committed to creating an open financial system for the world, and eagerly supports the best and smartest teams in the global encryption field to develop products and services that can create meaningful user and customer value. Coinbase Ventures is registered in the United States and is

committed to the investment and incubation of blockchain infrastructure on a global scale.

## Architecture

With an octa-core technology at its core, the HyperCube blockchain is both highly scalable and safe, as well as completely decentralized.

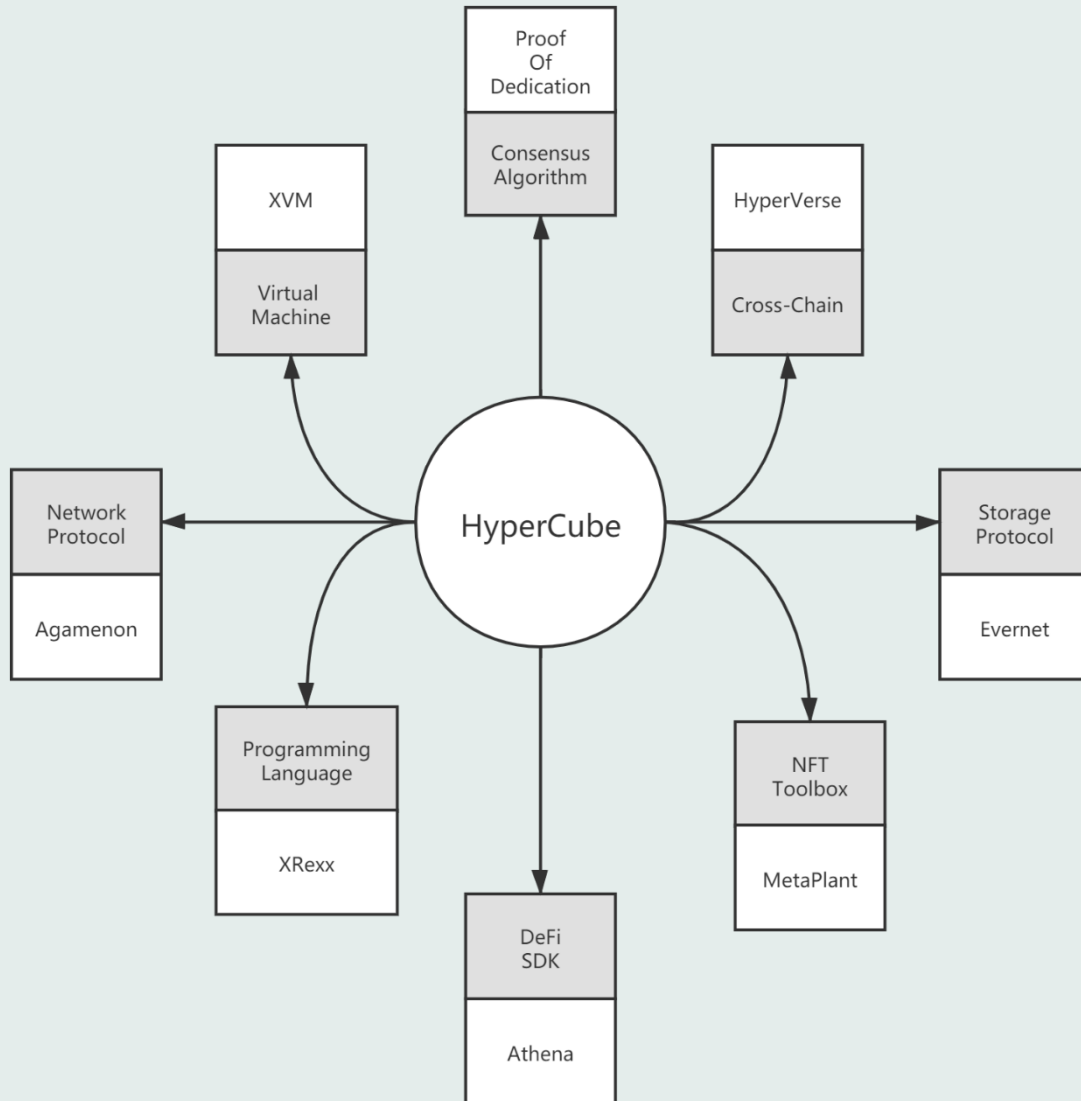


FIGURE 2 TECHNICAL ARCH

HyperCube is a hybrid PoW/PoS blockchain, which means that it relies on users to stake their XPZ tokens in order to become a certified miner on the network. Miners are paid to look through and verify transactions, and they do it in exchange for payments. When participating in a Hyper Pool, one alpha node is in charge of creating ledger entries; the likelihood of obtaining this job grows the more XPZ tokens a validator stakes.

Any particular miner node should never be the alpha node for an extended period of time; instead, an alpha node schedule limits each designated miner to 1 block until the next alpha node takes up the position.

## Proof of Dedication

### Existing Problems for Blockchain Consensus Algorithm

Blockchain was originally built for cryptocurrency, but we found that as the use of blockchain becomes more and more widespread, the scope of applications is also more and more extensive, it should be used to provide digital services in many business areas, including accounting And currency issuance. Its idea is: the idea of a computer platform that serves people all over the world. Only by creating a global infrastructure that serves all levels of development can blockchain technology be used in our daily lives.

However, in order to achieve the goal of having a global computing platform, there are two challenges to overcome: (1) Must include Turing completeness. Therefore, the program can only perform certain tasks if it has proper logical integrity. (2) Super Ability It was basically the same thing before, but now it's complicated, listening to music, playing games, and arranging things. If you want to accomplish more work, you must be able to accomplish several things at the same time.

The initial problem that Ethereum wants to solve is a breakthrough. After making Ethereum more humane for developers, the project realized Turing completeness and "smart contracts" before using the virtual machine EVM, providing project members with opportunities to interact with Ethereum more easily. Understand the specific needs of your business, complete the blockchain + deployment of your project, and use the underlying data. The bottom layer is the source of the anti-tampering function of the project.

The PoW (Proof of Work) consensus method used by Ethereum can only complete basic calculation work and storage capacity. With the rapid development of modern blockchains, innovations in practical applications of NFT and DeFi continue to emerge. The challenges faced by all new public blockchains are about performance: how to get better?

TPS is the core indicator that considers the underlying standards of the blockchain. TPS means how many pieces of data can be processed at the same time per second. At present, there are 24,000 Visa transactions, 100,000 stock transactions, and 250,000 Taobao transactions per second in the world. Shopping transactions, and at the same time, the cost and handling fee of each transaction relative to individual users can be ignored. As we face the blockchain world, the TPS of Ethereum is around 20, and the TPS of Bitcoin is 7. Therefore, in contrast, the expansion of the blockchain has become very important. The purpose of expansion

is not only to increase the transaction speed, but also to increase the single transaction fee. Pave the way for scale applications.

The proof of POD dedication proposed by the HyperCube team is to build a new generation of consensus protocol for the expansion of the blockchain from the protocol level.

## **Necessity to Expand the Ethereum**

HyperCube chooses Ethereum as the object of expansion, and defines PoD as a 2-layer solution that helps Ethereum improve processing speed and storage capacity.

This choice is because we realize that in addition to the improvement and expansion of the underlying technology, the success or failure of the blockchain system lies in the vast number of developers and the flourishing ecology. Ethereum is now the world's largest DAPP operating platform. , Has a wide range of and loyal developers and users. Therefore, the essence of commercial competition is traffic competition. We hope that POD can provide the most developers and the most blockchain users with a better experience.

## **POD Dedication To Prove How To Improve Computing Power**

As the infrastructure for DAPP development, the public chain only provides a fast and reliable foundation for DAPP. This will only provide a basis for creating killer applications. When comparing blockchain to the Internet, the first issue to discuss is its relative speed: its outstanding performance in processing data.

Blockchain technology must verify data upload. In short, in order to ensure the accuracy of the upload, the data must pass through all network nodes for parallel calculation, and then return to the network for data collection and verification. The latter process is definitely slower than centralized processing. Therefore, many people think that blockchain is a technology that sacrifices efficiency for security.

POD dedication proves that a balance between performance and decentralization is found. By combining sharding and staking, the definition of Value Of Dedication is proposed. Through the size of the dedication value, every In each block creation cycle, define who will verify and choose which data to write to the chain.

## **What Is The Difference Between POD Dedication Certificate And POW And POS**

PoW is the English abbreviation of the method used for proof of work. Under this algorithm, each network node in the network performs calculations at the same time, and the first person to obtain the correct answer will gain the ability to perform the next set of calculations. Therefore, a lot of meaningless waste will be generated. PoS depends on the age of the coin and the number of coins owned, as

well as some randomness to select those with longer coin age and more coins, and they are ultimately responsible for the information that joins the blockchain.

In the PoW consensus algorithm network, all network nodes participate in the calculation at the same time, and the person who calculates the result the fastest gets the accounting power. This process is essentially a calculation competition and zero-zero game. Machines with insufficient computing power consume electricity and time. , There will be no meaningful returns, and a lot of power resources are wasted.

The PoS is based on the age of the currency and the number of coins, plus some randomness, selects people with a longer coin age and a larger number of coins to obtain the verification power, and is ultimately responsible for putting the verified data on the chain. But so far, it is difficult for PoS to solve the problem of over-issued currency and the kidnapping of the community by large nodes.

POD proves consensus through dedication, and through reasonable selection of high-speed nodes for accounting, while taking into account performance, it also guarantees the high-speed performance of the network. This is like making a decision to choose a qualified president during a national election. If all the people of the whole country need to vote at the last minute, it will inevitably be slower to wait until the people of the whole country vote. However, adopting a similar proxy system and selecting a group of "reliable" people to choose the right president on behalf of the public can greatly improve the efficiency of the election.

## **D-Value**

The POD consensus mechanism describes an indicator for users of the entire network: D-Value. The quantitative consensus on dedication value is the consensus on the dynamic definition of multi-dimensional network proposed by HyperCube. D-Value is established based on the DAG transaction data model and social graph model of the directed acyclic graph. D-Value is used to quantify the contribution of nodes to the network, including computing power, time, storage and Multi-dimensional data such as community input.

Often the simplest and simplest ideas require the most complex and rigorous engineering methods to achieve. In the real society, everyone's social status depends on the value of his dedication to others. If a person has enough dedication to the family, he enjoys a high reputation in the family, and if he has dedication to the society, he has a lofty reputation in the society. Reputation. Contribution is the manifestation of an individual's value to others and the collective in the social organization structure. The more dedication, the more personal feedback will often

be, thus forming a positive cycle. The value of dedication includes the superposition of multiple factors such as group, labor, and creation. This invisible value determines the right to speak for individuals in the world. But it is the hidden value, so it is difficult to quantify it with models. Therefore, in HyperCube, we have realized the quantitative expression of the dedication system for the first time, using mathematical consensus to more accurately describe the existence value of a single individual in the entire organizational structure.

The emergence of POD is just like the emergence of POW. Using computer language to express the existence of individuals in social organizations, POW solves the credit value of labor, and POD takes it to a higher level. It not only expresses labor, but also expresses trust. , The credit value of existence and exchange.

## **Node Selection**

POD uses Byzantine fault tolerance, which analyzes possible nodes and their results before assigning nodes. In the first stage, all nodes will be evaluated and the 15% with the highest contribution will be randomly selected. This can be considered the "best" node in the network. In contrast, the maximum number of nodes allowed in the node pool is 1000 and the minimum is 100. In order to ensure that the transaction passes Byzantine Fault Tolerance (PFDT), you need to randomly select nodes in the "node candidate pool". After that, a selected node checks the transaction of the network and puts the confirmed transaction on the chain.

By using a collective decision-making process, the strategy aims to combat election bribery and provides a "choice of good nodes" procedure that will verify a limited range of data while being efficient and decentralized.

## **Factors of D-Value**

D-Value is determined according to the HyperCube network dynamic equilibrium formula, and it will keep changing at every moment. The nodes participating in the formula must want to obtain a high D-Value, and must strengthen the node configuration in the following aspects

### **Stake Holding**

All HyperCube nodes must be pledged to start using XPZ tokens. The more the number of tokens pledged by the node, the longer the pledge time, and the larger the D-Value will be.

### **Network**



In the HyperCube network, there will be backbone nodes and verification nodes. After being filtered by D-Value, a backbone node will be formed, and all nodes will communicate and exchange data with the backbone node. In this process, the smoother the communication, the higher the D-Value.

At the same time, if the node goes offline, D-Value will be greatly reduced

## **Hardware**

HyperCube will determine the contribution value of the node to the network based on the CPU core, GPU core, hard disk space, RAM space and other multi-dimensional factors.

## **Community**

HyperCube supports the entire SPS ecosystem, and users with SPS tokens can get a higher D-Value. Considering the number of users who have strong social connections with each other on HyperCube, how often they interact with friends, their dedication to each other, and the volume of transactions between them, it can be determined that this node will be very advantageous in the competition of the bookkeeping node, Will get higher rewards. If you are a high-profile project party on HyperCube, a key opinion leader (KOL) who often interacts with fans, or a community leader with excellent operational capabilities, then D-Value rewards may be very beneficial to your account balance.

## Network

When communicating with nodes in the control plane, the MINO Protocol (MINO) is used as a gateway. The service is used by miners to ensure that information is available to all other nodes in a cluster of computers. The MINO protocol is used by the service to disseminate information.

### Protocol Overview

It is necessary for nodes to transfer signed data objects among themselves in order to run a cluster on an ongoing basis. They may, for example, share their contact information, ledger height, and voting preferences with others. Every tenth of a second, each node transmits a "push" message and/or a "pull" message to the rest of the network. It is possible that push and pull messages will elicit answers, and that push messages will be forwarded on to other nodes in the cluster as well. MINO runs on a well-known UDP/IP port, or on a port in a well-known range, and it is easy to remember. Once a cluster has been booted up, nodes communicate with one another about where to find their MINO endpoint (a socket address).

### MINO Records

It is not necessary to sign or version (with a date) records shared over MINO in order for them to be understandable by the node that is receiving them. Whenever a node receives two records from the same source, it replaces the oldest record with the most recent record with the latest timestamp.

### MINO Interface

#### PUSH MESSAGE

A node sends a push message to tell the cluster it has information to share. Nodes send push messages to PUSH\_FANOUT push peers.

#### PUSH PEERS, PRUNE MESSAGE

A node selects its push peers at random from the active set of known peers. The node keeps this selection for a relatively long time. When a prune message is received, the node drops the push peer that sent the prune. Prune is an indication that there is another, higher stake weighted path to that node than direct push. The set of push peers is kept fresh by rotating a new node into the set every PUSH\_MSG\_TIMEOUT/2 milliseconds.

## **PULL MESSAGE**

A node sends a pull message to ask the cluster if there is any new information. A pull message is sent to a single peer at random and comprises a Bloom filter that represents things it already has. A node receiving a pull message iterates over its values and constructs a pull response of things that miss the filter and would fit in a message.

A node constructs the pull Bloom filter by iterating over current values and recently purged values. A node handles items in a pull response the same way it handles new data in a push message.

## **PURGING**

Nodes retain prior versions of values (those updated by a pull or push) and expired values (those older than `MINO_PULL_BLACKTHRD_TIMEOUT_MS`) in `purged_values` (things I recently had). Nodes purge `purged_values` that are older than  $5 * \text{AGMN\_PULL\_BLACKTHRD\_TIMEOUT\_MS}$ .

## Tokenomics

The overall supply of tokens is deflationary. HyperCube's token economic structure is designed according to the standards of deflation and security maintenance, and the purpose is to maintain the most secure economic structure of the network system while maintaining a reasonable supply of tokens.

The HyperCube crypto-economic system is intended to promote a healthy, long-term, self-sustaining economy by aligning participant incentives with network security and decentralization. Validation-clients are the primary participants in this economy. Their network contributions, state validation, and the necessary incentive mechanisms are discussed further below.

Protocol-based rewards and transaction fees are the two main channels of participant remittances. Protocol-based rewards are created by issuing inflationary issuances according to a protocol-defined inflation schedule. The total protocol-based reward delivered to validation clients will be comprised of these rewards, with the remainder sourced from transaction fees. Protocol-based rewards, deployed on a predefined issuance schedule, are likely to drive the majority of participant incentives to participate in the network in the network's early days.

These protocol-based rewards are calculated and distributed per epoch across the active delegated stake and validator set (per validator commission). The annual inflation rate is determined by a predetermined disinflationary schedule, as discussed further below. This provides supply predictability to the network, which supports long-term economic stability and security.

Transaction fees are participant-to-participant transfers that are attached to network interactions as motivation and compensation for the inclusion and execution of a proposed transaction. A mechanism for long-term economic stability and forking protection is also discussed below, involving the partial burning of each transaction fee.

First, a high-level overview of the inflation design is provided. This section begins by defining and clarifying terminology commonly used in discussions of inflation and its constituents.

Then, we outline HyperCube's proposed Inflation Schedule, which includes the specific parameters that uniquely parameterize the protocol-driven inflationary issuance over time.

Following that is a brief discussion of Adjusted Staking Yield and how token dilution may affect staking behavior.

An overview of Transaction Fees on HyperCube is followed by a discussion of Storage Rent Economics, in which we describe the implementation of storage rent to account for the externality costs of maintaining the active state of the ledger.

## **Terminology**

### **Current Supply Cap**

The total number of tokens (locked or unlocked) generated (via genesis block or protocol inflation) less any tokens burned (via transaction fees or other mechanism) or slashed.

210,000,000 XPZ were instantiated in the genesis block at network launch. The Current Supply Cap is subject to reduction since then as a result of the burning of transaction fees and a planned token reduction event.

### **Inflation Index**

The HyperCube protocol will generate new tokens based on a predetermined inflation schedule (discussed below). The annualized growth rate of the Current Supply Cap at any point in time is represented by the Inflation Index [ % ].

### **Supply Time Table**

A time-dependent deterministic description of token issuance. A dis-inflationary inflation schedule is proposed by the HyperCube Protocol. In other words, inflation begins at its highest level and gradually decreases until it reaches a predetermined long-term inflation rate (see discussion below). Three numbers completely and uniquely parameterize this schedule:

- Initial Inflation Index [%]: The starting Inflation Rate for when inflation is first enabled. Token issuance rate can only decrease from this point.
- Deflation Index [%]: The rate at which the Inflation Rate is reduced.
- Long-term Inflation Index [%]: The stable, long-term Inflation Rate to be expected.

## Viable Inflation Index

After accounting for other factors that could reduce the Current Supply Cap, the inflation index observed on the HyperCube network. It should be noted that tokens cannot be created outside of the parameters specified in the **Supply Time Table**.

- While the **Supply Time Table** governs how the protocol distributes XPZ, it ignores the concurrent elimination of tokens in the ecosystem due to a variety of factors. The burning of a portion of each transaction fee is the primary token burning mechanism. Half of each transaction fee is burned, with the remaining fee kept by the miner who processes the transaction.
- Other factors, such as the loss of private keys and slashing events, should be considered in a comprehensive analysis of the Viable Inflation Index. For example, it is estimated that 10% of all BTC has been lost and is unrecoverable, and that networks may experience similar yearly losses of 1 - 2%.

## Staking Yield [%]

The rate of return (aka interest) earned on XPZ staked on the network. It is often quoted as an annualized rate (e.g. "the network staking yield is currently %10% per year").

The rate of return (also known as interest) on XPZ staked on the network. It is frequently expressed as an annualized rate (e.g. "the network staking yield is currently percent 10 percent per year").

- Validators and token holders who want to delegate their tokens to avoid token dilution due to inflation are particularly interested in staking yield (the extent of which is discussed below).
- 100% of inflationary issuances will be distributed to staked token holders in proportion to their staked XPZ, as well as validators who will charge a commission on the rewards earned by their delegated XPZ.
  - With the introduction of Evernet Keeper into the economy, there may be future consideration for an additional split of inflation issuance.

- Evernet Keepers are network participants who provide a decentralized storage service and should be rewarded with token distributions from inflation issuances in exchange for this service.
- Similarly, early concepts called for a fixed percentage of inflationary issuance to be delivered to the Foundation treasury for operational expenses and future grants.
- Inflation, on the other hand, will begin without any funds allocated to the Foundation.
- The Supply Time Table, along with the fraction of the Current Supply Cap staked at any given time, can be used to calculate staking yield. The following expresses the explicit relationship:

$$Y_{staking} = \frac{i_{inflation} \times T_{valid} \times XPZ_{Total}}{XPZ_{staked}} \times (1 - fee_{miner})$$

### Token Dilution [%]

Dilution is defined as a change in the proportional representation of a set of tokens within a larger set as a result of the introduction of new tokens.

In practice, we talk about the dilution of staked or un-staked tokens as a result of the introduction and distribution of inflation issuance across the network. While dilution affects all token holders, the relative dilution between staked and un-staked tokens should be of primary concern to un-staked token holders, as shown below. Staking tokens, which will receive their proportional distribution of inflation issuance, should alleviate staked token holders' concerns about dilution.

In other words, the dilution caused by 'inflation' is offset by the distribution of new tokens to staked token holders, effectively canceling out the 'dilutive' effects of the inflation for that group.

### Adjusted Staking Yield [%]

A complete assessment of the earning potential of staking tokens should consider staked Token Dilution and its impact on the Staking Yield. We define the Adjusted Staking Yield as the change in fractional token supply ownership of staked tokens

as a result of inflation issuance distribution. In other words, the positive dilutive effects of inflation.

## Supply Time Table

As previously stated, the network's Supply Time Table is uniquely described by three parameters: Initial Inflation Index, Deflation Index, and Long-term Inflation Index. Many factors must be considered when analyzing these figures:

A large portion of the XPZ issued through inflation will be distributed to XPZ miners in proportion to the XPZ staked. We want to make sure that the Supply Time Table design results in reasonable Staking Yields for token holders who delegate XPZ and validation service providers (via commissions taken from Staking Yields).

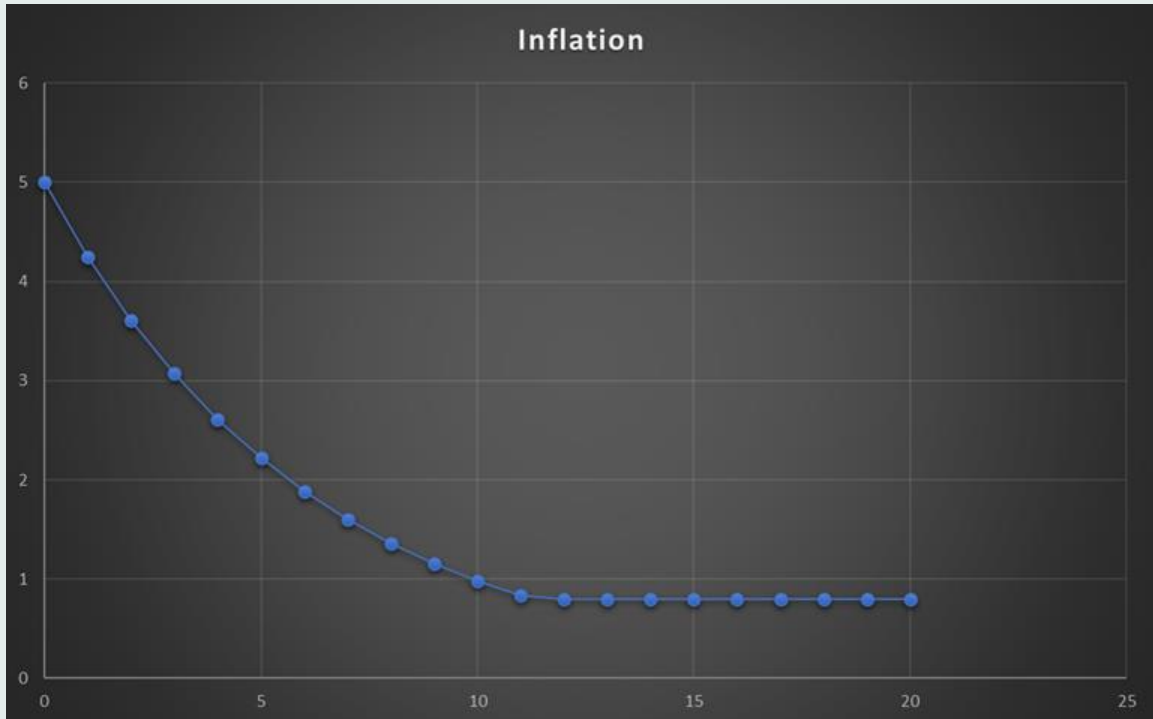
The primary determinant of Staked Yield is the amount of XPZ staked divided by the total amount of XPZ ( percent of total XPZ). As a result, when determining initial inflation parameters, it is critical to understand the distribution and delegation of tokens across validators.

Yield throttling is a current area of research that could have an impact on staking-yields. This is not taken into account in the discussion or modeling below. Overall token issuance - i.e., what do we expect the Current Total Supply to be in 10 years or 20 years? Long-term, steady-state inflation is an important consideration not only for long-term support for the validator ecosystem and the Solana Foundation grant programs, but it should also be tuned in consideration of expected token losses and burning over time. The rate at which we expect network usage to grow in relation to the disinflationary rate. We expect inflation to fall over time and usage to rise. Based on these considerations and the community discussions that followed the initial design, the Solana Foundation proposes the following Inflation Schedule parameters:

- Initial Inflation Index: 8%
- Deflation Index: 15%
- Long-term Inflation Index: 0.8 percent



These parameters define the proposed Inflation Schedule. The consequences of these parameters are shown below. These plots only show the impact of inflation issuances given the Inflation Schedule as parameterized above. They do not take into account other factors that may have an impact on Total Supply, such as fee/rent burning, slashing, or other unforeseen future token destruction events. As a result, what is presented here is an upper limit on the amount of XPZ issued through inflation.



In the above graph we see the annual inflation rate [%] over time, given the inflation parameters proposed above.



Similarly, we can see the Circulating Supply Cap of XPZ [MM] over time, assuming an initial Circulating Supply Cap of 488,587,349 XPZ (i.e. for this example, taking the Circulating Supply Cap as of 2020-01-25 and simulating inflation starting from that day).

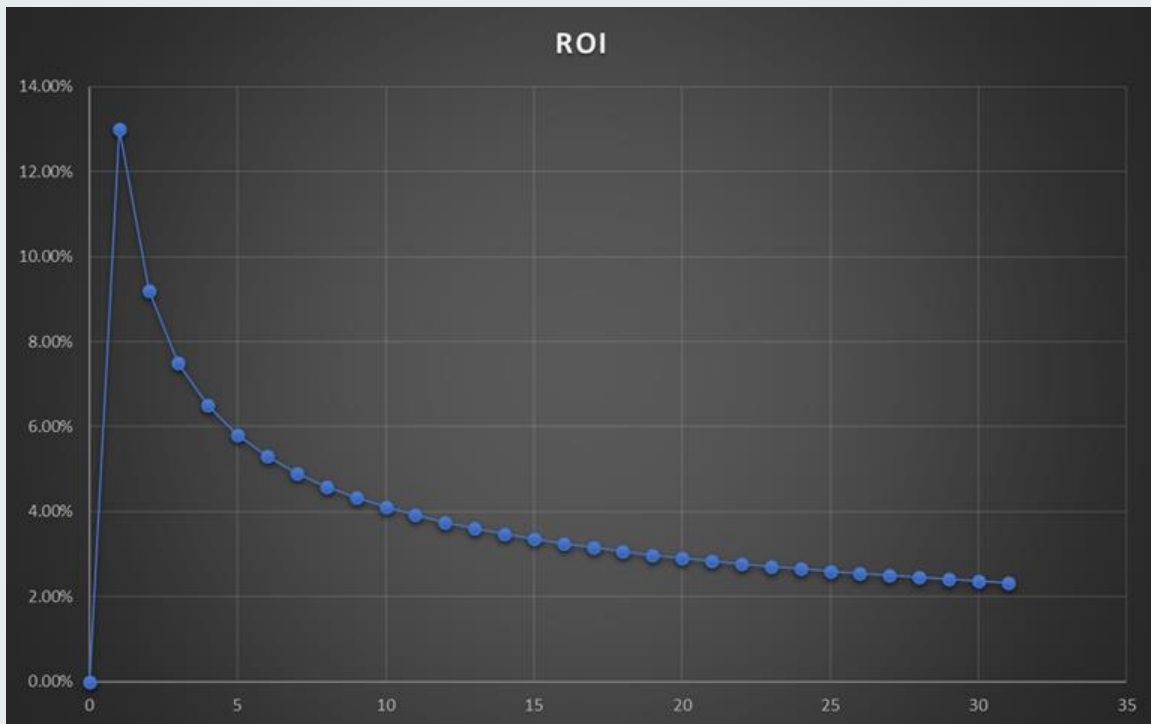
When validator uptime and commissions are taken into account, the expected Staking Yield and Adjusted Staking Yield metrics are essentially a function of the percent of total XPZ staked on the network. As a result, if we add an additional parameter percent of Staked XPZ, we can model Staking Yield:

$$S_r = \frac{XPZ_{staked}}{XPZ_{cap}} \times 100\%$$

Where  $S_r$  stands for the percentage of the staked XPZ in the total supply.

Because it is a dynamic characteristic of token holders and staking incentives, this parameter must be calculated. Based on comments from the investor and validator communities, as well as what is observed on analogous Proof-of-Stake protocols,

the percent of Staked XPZ shown here ranges from 60% to 90%, which we believe represents the likely range we expect to see.



Again, with the Supply Time Tables supplied, the following displays an example Staked Yield that a staker can expect over time on the HyperCube network. This is a skewed Staked Yield since it ignores the influence of validator downtime on rewards, validator commissions, potential yield throttling, and potential slashing occurrences. It also ignores the fact that the percent of Staked XPZ is dynamic by design - the economic incentives established by this Supply Time Table are more clearly seen when Token Dilution is included (see the Adjusted Staking Yield section below).

## Tailored Staking Yield

### Token Dilution

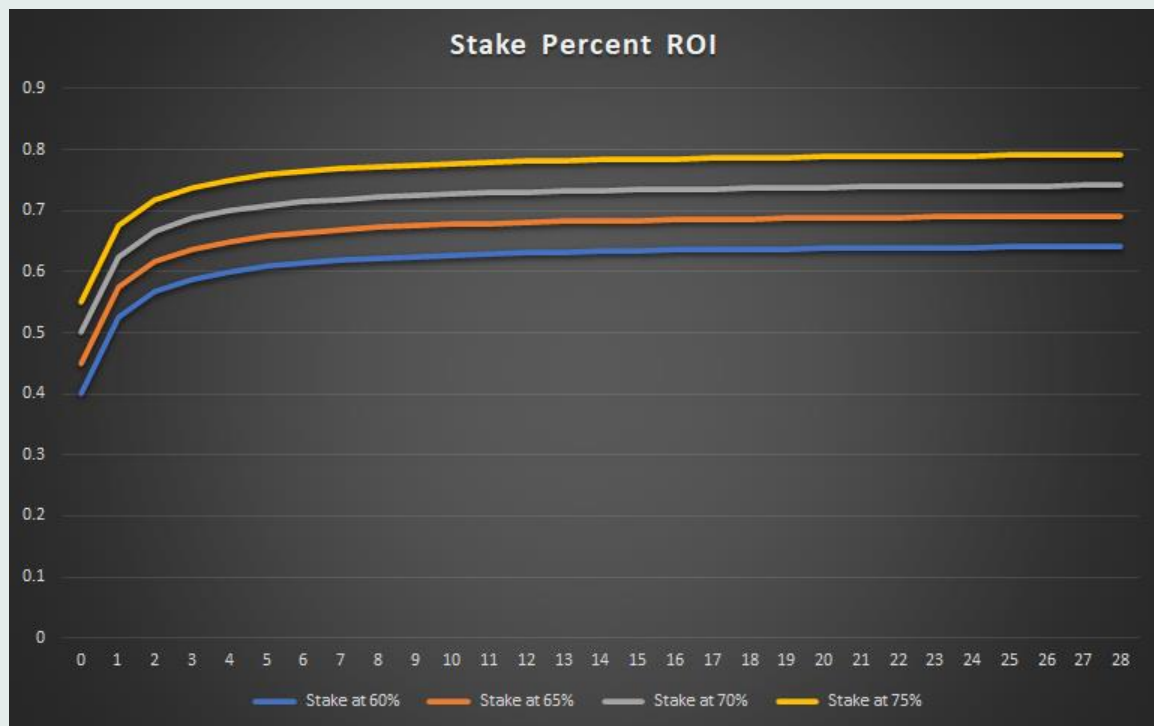
As previously defined, we can look at the predicted Staked Dilution (i.e. Tailored Staking Yield) and Un-staked Dilution. The change in fractional representation (i.e. ownership) of a set of tokens inside a bigger set is characterized as dilution in this context. In this meaning, dilution can be a positive or negative value: an increase in

fractional ownership (staked dilution / Tailored Staking Yield) or a decrease in fractional ownership (staked dilution / Tailored Staking Yield) (un-staked dilution).

As the general token pool grows with inflation supply, we're interested in the relative change in ownership of staked vs un-staked tokens. As previously stated, only staked token holders would receive this issuance, raising the staked token fractional representation of the Current Supply Cap.

Using the same Supply Time Table parameters as before, the fraction of staked supply grows as indicated in the graph below.

### Growth of Staked Supply



Due to this relative change in representation, the proportion of stake of any token holder will also change as a function of the Inflation Schedule and the proportion of all tokens that are staked.

Of initial interest, however, is the dilution of un-staked tokens, or  $D_{us}$ . In the case of un-staked tokens, token dilution is only a function of the Inflation Schedule because the amount of un-staked tokens doesn't change over time.

This can be seen by explicitly calculating un-staked dilution as  $D_{us}$ . The un-staked proportion of the token pool at time  $t$  is  $P_{us}(t_N)$  and  $I_t$  is the incremental inflation rate applied between any two consecutive time points.

$XPZ_{us}(t)$  and  $XPZ_{total}(t)$  is the amount of un-staked and total XPZ on the network, respectively, at time t. Therefore.

$$P_{us}(t) = \frac{XPZ_{us}(t)}{XPZ_{total}(t)}$$

$$D_{us}(t) = \frac{P_{us}(t_1) - P_{us}(t_0)}{P_{us}(t_0)}$$

$$D_{us} = \frac{\frac{XPZ_{us}(t_2)}{XPZ_{total}(t_2)} - \frac{XPZ_{us}(t_1)}{XPZ_{total}(t_1)}}{\frac{XPZ_{us}(t_1)}{XPZ_{total}(t_1)}}$$

However, because inflation issuance only increases the total amount and the un-staked supply doesn't change:

$$XPZ_{us}(t_2) = XPZ_{us}(t_1)$$

$$XPZ_{total}(t_2) = XPZ_{total}(t_1) \times (1 + I_{t_1})$$

So  $D_{us}$  becomes:

$$D_{us} = \frac{\frac{XPZ_{us}(t_1)}{XPZ_{total}(t_1) \times (1 + I_i)} - \frac{XPZ_{us}(t_1)}{XPZ_{total}(t_1)}}{\frac{XPZ_{us}(t_1)}{XPZ_{total}(t_1)}}$$

$$D_{us} = \frac{1}{1 + I_i} - 1$$

Or generally, dilution for un-staked tokens over any time frame undergoing inflation  $I$  :

$$D_{us} = -\frac{I}{I + 1}$$

So as guessed, this dilution is independent of the total proportion of staked tokens and only depends on inflation rate. This can be seen with our example Supply Time Table here:

## Mining

HyperCube introduces miners to process data on the blockchain. Miners are essentially home computers that are responsible for publishing, signing, and storing blocks.

### Hardware Specification

#### Generic Requirement

- *CPU: 8 Core Or More, 2.0 GHZ Or Faster*

To mine, you'll need a high-end CPU, at least 8 cores. We would really encourage a model that supports Intel SHA Extensions: Zen for AMD, or Ice Lake for Intel. A substantial slowdown is caused by the lack of SHA Extensions.

- *RAM: 128 GB Or More*

At the absolute minimum, you will need 128 GB of RAM. On an extremely fast NVMe SSD storage medium, you should also have 256 GiB of swap for extra space.

- *Disk: 1TB or More*

Miner activities can be hindered by slower drives, which can result in their performance issues. In one instance, a 32GiB drive was increased to about 480GiB. The HyperCube network's 100 GiB of settings must be read and confirmed in order to activate the Miner. Above, you'll remember we discussed how RAM issues have to be handled by way of an exceptional swap disk or an efficient file system.

We advise that, to avoid storing frequently accessed content in cache more than necessary, at least 1TiB of NVMe cache space should be allotted. HyperCube parameters and other general data should be stored on this disk, as it's needed for caching data during the sealing process.

- *GPU: 1660s with 6GB Memory or Better*

A powerful GPU is recommended as it can significantly speed up SNARK computations.

#### Whitelabel Machine

We have provided a list of thoroughly tested rig spec which will highly increase the output of miner machine. Usually miner rigs in the white list are usually much superior in terms of output.

## Cloud Mining

It is feasible to run a HyperCube miner on the cloud, although it is much cost-efficient to run a bare metal.

## Mining Collateral

In order to participate in the consensus process, the vast majority of permissionless blockchain networks necessitate an initial expenditure of resources. The greater the influence an entity has on the network, the greater the share of total resources it is required to own, whether in the form of real assets or staked tokens, in order to maintain that influence (collateral).

It is necessary for HyperCube to achieve security through resource allocation. Due to the fact that HyperCube mining employs just commercial hardware (as opposed to ASIC technology) that is inexpensive to amortize and easily recycled, the protocol cannot rely solely on the hardware as the capital investment at stake for attackers, as would be the case with ASIC technology. Additionally, HyperCube makes use of upfront token collaterals, similar to proof-of-stake systems, that are equal to the amount of storage hardware that has been committed to the project.

Thus, you have the ideal combination: in order to attack a network, not only must the hardware be purchased, but also large numbers of the token must be purchased in order for the attack to be successful.

HyperCube contains two unique collateral systems to satisfy the multiple collateral requirements while lowering the load on miners to a bare minimum.

Among the three types of collateral are

Type 1: collateral for the initial pledge,

Type 2: collateral for the block reward, and

Type 3: collateral for the hardware rigger.

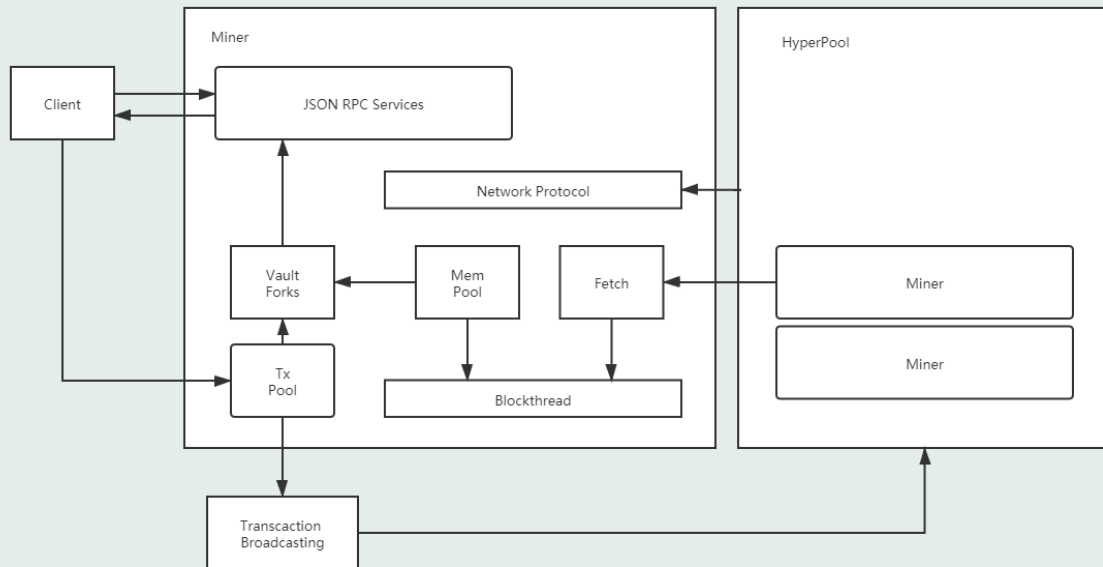
The first is a one-time HyperCube commitment that a miner must make for each sector in which they are participating.

The second is a mechanism for minimizing the initial token investment by allowing block rewards to be progressively vested over time.

The third option attempts to strike a balance between the motivations of hardware riggers and miners, potentially allowing miners to distinguish themselves in the

market. The remainder of this section goes into deeper depth on each of these topics..

## Mining Processing Pipeline



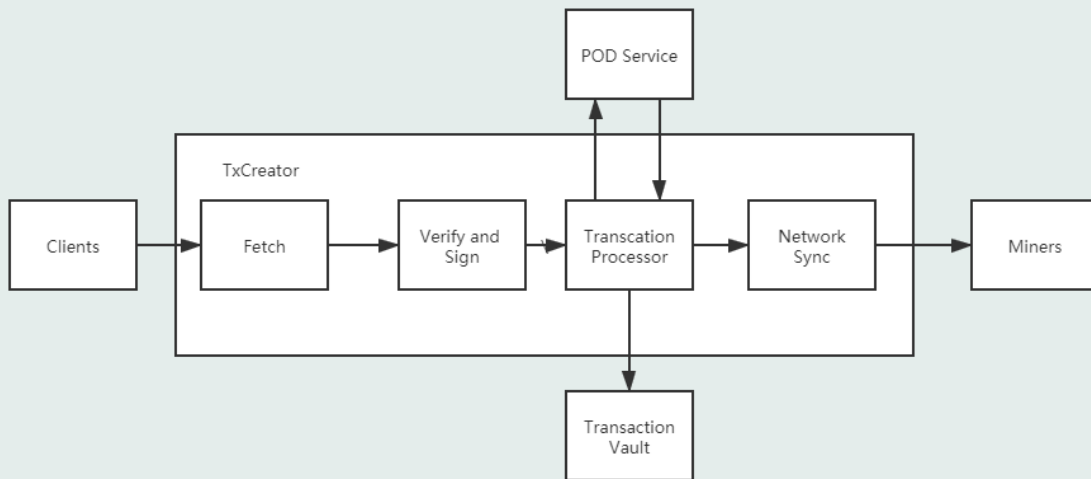
The miners extensively use pipelining, which is prevalent in CPU architecture. If there's a stream of input data that must be processed through a sequence of steps, and distinct hardware is accountable for each, the tool that will best suit the task is pipeline. An exemplary usage would be doing multiple loads of laundry by washing, drying, and folding everything in a washer and dryer. One machine dries, one machine folds, and another machine washes. To increase productivity, it is important to design a staged pipeline. We'll classify the washer, dryer, and folding procedure as different stages of the folding process. You finish a load of laundry by adding a second load to the washer after it has been put in the dryer. Next, after the second load has finished drying and the first is being folded, the third is being put in the washer. It's possible to do three loads of laundry all at once if one goes about it like this. On a day when the pipeline has to process an unlimited number of loads, the pipeline will finish every load at the speed of the slowest step in the pipeline.

A total of two processes in the miner are pipelined: the TxCreator works in leader mode, and the TxSigner works in miner mode. There is no difference in hardware

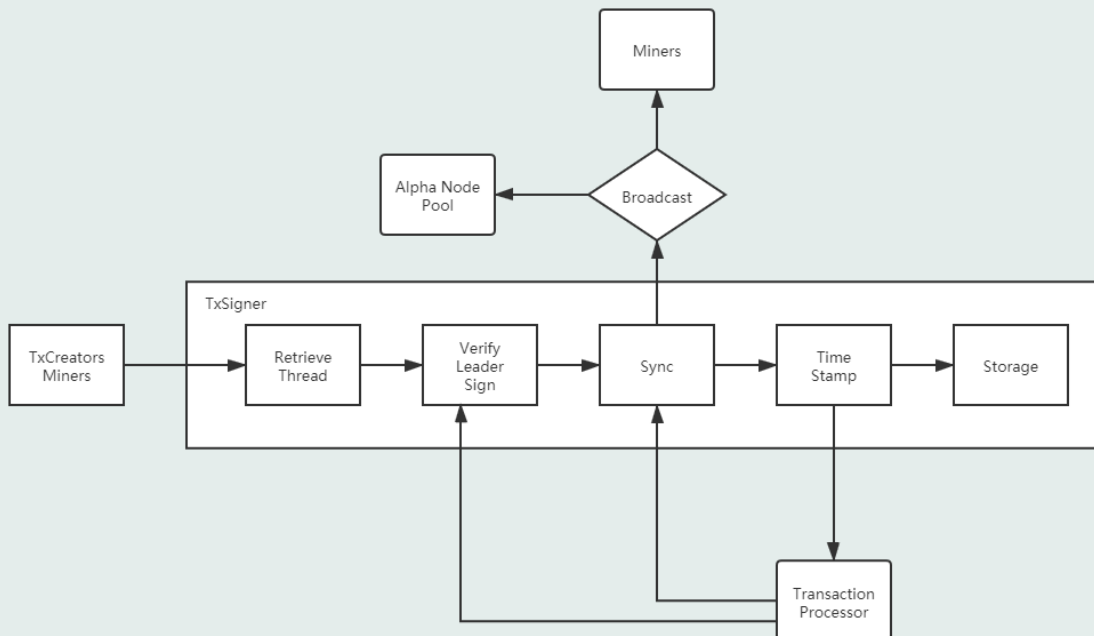


and the equipment which is pipelined for both sets of scenarios: network input, GPU cards, CPU cores, disk writing, and network output. What it does is unlike the competition. The TxCreator's purpose is to produce entries in the ledger, whereas the TxSigner's is to confirm them.

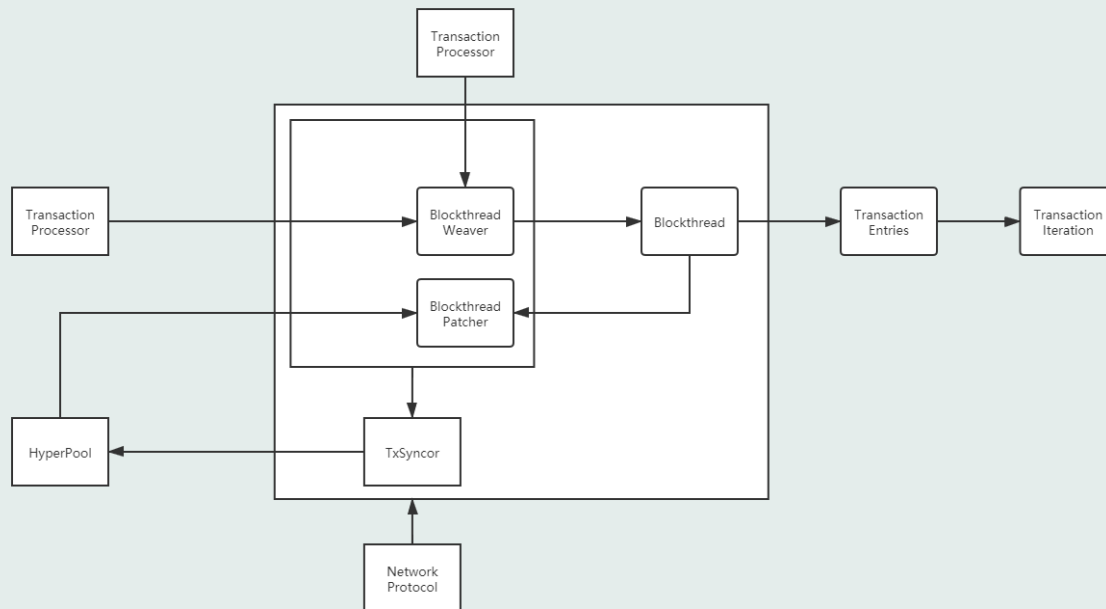
## TxCreator



## TxSigner



## TxSyncor



## HyperPool

A HyperPool is a group of miners who collaborate to serve client transactions while maintaining the ledger's integrity. Several pools may coexist. When two pools share a genesis block, they make an attempt to converge. Otherwise, they simply ignore the other's existence. Transactions sent to the incorrect address are quietly rejected. In this section, we'll go over how to create a pool, how nodes join the pool, how they share the ledger, how they ensure the ledger is replicated, and how they deal with buggy and malicious nodes.

### Constructing a HyperPool

Before starting any miners, a genesis config must be created. The configuration makes use of two public keys, a mint and a bootstrap miner. The miner in possession of the bootstrap miner's private key is in charge of appending the first entries to the ledger. It loads the mint's account into its internal state. That account will contain the number of native tokens specified in the genesis configuration. After that, the second miner contacts the bootstrap miner to register as a miner. Additional miners can then register with any registered pool member.

A miner receives all entries from the leader and votes to confirm the validity of those entries. The miner is expected to save the votes after they have been cast.

When the miner notices that there are a sufficient number of copies, it deletes its copy.

## **Becoming a member of a HyperPool**

Miners join the pool by sending registration messages to the pool's control plane. The control plane is implemented using a gossip protocol, which means that a node can register with any existing node and expect its registration to be broadcast to all nodes in the pool. The time it takes for all nodes in the pool to synchronize is proportional to the square of the number of nodes in the pool. That is considered very slow algorithmically, but in exchange for that time, a node is assured that it will eventually have all of the same information as every other node, and that that information cannot be censored by any single node.

## **Transacting with a HyperPool**

Clients send transactions to the Transaction Processing Unit (TPU) port of any miner. If the node is acting as a miner, it sends the transaction to the designated leader. If the node is in the leader role, it bundles incoming transactions, timestamps them, creates an entry, and pushes them onto the data plane of the pool. Once on the data plane, miner nodes validate the transactions, effectively appending them to the ledger.

## **Transaction Confirmation**

A HyperCube pool can confirm transactions in subseconds for up to 150 nodes, with plans to scale up to hundreds of thousands of nodes. Once fully implemented, confirmation times are expected to increase only in proportion to the logarithm of the number of miners, where the base of the logarithm is very large. If the base is one thousand, for example, it means that confirmation will take three network hops plus the time it takes the slowest miner in a supermajority to vote for the first thousand nodes. Confirmation increases by one network hop for the next million nodes.

According to HyperCube, confirmation is the period of time between when the leader timestamps a new entry and when it recognizes a supermajority of ledger votes.

Once a gossip network reaches a certain size, it becomes far too slow to achieve subsecond confirmation. The time it takes to send messages to all nodes is proportional to the number of nodes multiplied by the square of the number of

nodes. If a blockchain wants to achieve low confirmation and uses a gossip network, it will be forced to centralize to a small number of nodes.

Scalable confirmation can be achieved by combining the following techniques:

- Sign the timestamp and timestamp transactions with a VDF sample.
- Divide the transactions into batches, send each to a different node, and have
- Each node distributes its batch to its peers.
- Repetition the previous step until all nodes have all batches.

HyperCube rotates leaders at predetermined intervals known as slots. Each leader may only submit entries during the time allotted to them. As a result, the leader timestamps transactions so that miners can look up the designated leader's public key. The leader then signs the timestamp so that a miner can verify it, proving that the signer is the owner of the designated leader's public key.

Following that, transactions are divided into batches so that a node can send transactions to multiple parties without having to duplicate them. If the leader needed to send 60 transactions to six nodes, it would divide the collection into batches of ten transactions and send one to each node. This enables the leader to send 60 transactions over the wire rather than 60 transactions for each node. Each node then distributes its batch to its peers. Once all six batches have been collected, the node reconstructs the original set of 60 transactions.

A batch of transactions can only be split so many times before the header information consumes the majority of network bandwidth. At the time of writing, the approach has scaled up to about 150 miners. To scale to hundreds of thousands of miners, each node can apply the same technique as the leader node to another set of equal-sized nodes. Turbine Block Propagation is the name we give to this technique.

## Alpha Node

A hyperpool expects only one miner to produce ledger entries at any given time. Because only one alpha node is active at a time, all miners can replay identical copies of the ledger. The disadvantage of only running one alpha node at a time is that a malicious alpha node can censor votes and transactions. Because censoring cannot be distinguished from network packet loss, the hyperpool cannot simply elect a single node to serve as the alpha node indefinitely. Instead, the hyperpool reduces the impact of a malicious alpha node by alternating which node takes the lead.

Each miner employs the same algorithm, which is described below, to select the expected alpha node. When the miner receives a new signed ledger entry, it can be confident that it was generated by the anticipated alpha node. An alpha node schedule is the order in which each alpha node is assigned a slot.

## Rotation

Blocks that are not signed by the slot alpha node are rejected by a miner. A slot alpha node schedule (alpha node schedule) is a list of all the IDs of the slot alpha nodes. Locally and every now and then, the alpha node scheduling is recomputed. Epochs last for a time that gives the assignment of alpha nodes for slot variables. In order to do their jobs properly, the work being done on the ledger must be completely finished before it can be scheduled to start. Alpha node schedule offset is the name of that duration. Solana establishes the time difference for slot durations until the next epoch. The alpha node schedule for an epoch is defined at the start of the preceding epoch, based on the ledger state. The amount of time between each epoch is assumed to be long enough for all miners to be finished before the next schedule is created. To help minimize the time between stake changes and alpha node schedule updates, a hyperpool may decide to reduce the offset.

There is no need to build a schedule unless the root fork passes the epoch limit. The root fork is planned for the next epoch, therefore the new roots won't be in use until then. The first block of epoch 0 that the node schedule crosses belongs to epoch 0.

Without a partition lasting longer than an epoch, the hyperpool will work as follows:

- A miner continuously updates its own root fork as it votes.
- The miner updates its alpha node schedule each time the slot height crosses an epoch boundary.

For example:

To make things simpler, assume an epoch length of 100 slots, even if it's in reality much larger. The root fork is moved to a new slot at a height of 102, which is from a slot height of 99. Due to errors, slots at height 100 and 101 were skipped. The slot height 102 bifurcation is the starting point for the new alpha node schedule. Until it is updated again, it is active from slot 200.

If a miner on the hyperpool votes for a different candidate than the majority of miners, then their current candidate's vote on issue 101 will be rendered

meaningless. Every miner would have to commit to a root, either 102 or its descendent.

## **Alpha Node Schedule Rotation with Epoch Sized Partitions**

The alpha node schedule is vulnerable to error when the alpha node schedule has an inconsistent view of the actual alpha node schedule because of the duration of the alpha node schedule offset.

Picture this:

A couple of dividers with each one making half of the blocks. There will be no clear big bifurcation in either of them. Both of these will jump into the first two hundred generations without committing to the root or changing the new alpha node timetable for the hyperpool.

In this uncertain situation, several feasible plans for alpha nodes exist.

- A alpha node schedule is generated for every fork whose direct parent is in the previous epoch. The alpha node schedule is valid after the start of the next epoch for descendant forks until it is updated.
- Each partition's schedule will diverge after the partition lasts more than an epoch. For this reason, the epoch duration should be selected to be much much larger than slot time and the expected length for a fork to be committed to root.

To find a suitable alpha node scheduling offset, the hyperpool should be watched for a long period, and then the interval should be based on the median partition duration and its standard deviation. For instance, for instance, a tolerance which is more than 6 standard deviations above the average length of a partition means that in a hyperpool the risk of a corrupt ledger schedule is 1 in 1 million.

## **Alpha Node Schedule Generation at Genesis**

The configuration file sets the first epoch's first node as its beginning. Because the alpha node schedule is likewise generated at slot 0 for the next epoch, the alpha node is planned for the first two epochs. You can specify the duration of the first two epochs in the genesis config. POD BFT defines the maximum rollback depth; the earliest epochs should have a minimum length that exceeds or equals that maximum.

alpha node Schedule Generation Algorithm

In order to make scheduling of Alpha Node seed easy, a predetermined seed is used. Here is the process:

- The PoD tick height (a monotonically growing counter) can be used to seed a pseudo-random process, and can be used at regular intervals.
- It is recommended that each proxy node run a few network transaction consistency checks before moving onto the next task. For instance, the node can make sure to scan the network to discover all staked identities. The term "active set" describes the sample.
- Sort the people with the greatest impact on the problem into the critical set.
- Use the random seed to select nodes weighted by stake to create a stake-weighted ordering.
- This ordering becomes valid after a hyperpool-configured number of ticks.

## **Schedule Attack Vectors**

### Seed

Seed selection is not biased or predictable. No grinding attack to affect the outcome exists.

### Active Set

By suppressing miner votes, an alpha node can skew the active set. Alpha nodes can censor the active set in two ways:

- Ignore votes from miners
- Refuse to vote for blocks with votes from miners

The active set is calculated at the alpha node schedule offset border over an active set sampling length to minimise the possibility of censorship. The active set sampling duration is long enough that many alpha nodes will have collected votes.

### Staking

Alpha Nodes have the ability to censor new staking transactions or refuse to validate blocks containing new stakes. This attack is comparable to miner vote censorship.

### miner operational key loss

Alpha Nodes and miners are supposed to operate using ephemeral keys, and stake owners permit miners to execute work with their stake through delegation.

The hyperpool should be able to recover from the loss of all ephemeral keys used by alpha nodes and miners, which could happen as a result of a common software flaw shared by all nodes. Even though the stake is currently assigned to a miner, stake owners should be able to vote directly by co-signing a miner vote.

## **Appending Entries**

An epoch is the duration of an alpha node schedule. The epoch is divided into slots, each with a duration of T POD ticks.

During its slot, an alpha node sends entries. All miners switch to the next planned alpha node after T ticks. Miners must disregard entries received outside of an alpha node's allotted slot.

The following alpha node must witness all T ticks in order to create its own entries. If no entries are noticed (the alpha node is down), or if the entries are invalid (the alpha node is buggy or malicious), the following alpha node must supply ticks to fill the prior alpha node's slot. It should be noted that the next alpha node should do repair requests in parallel and delay delivering ticks until it is satisfied that other miners did not observe the previous alpha node's contents. If an alpha node builds wrongly on its own ticks, the alpha node that follows it must replace all of its ticks.

## **Miners Sync**

Fast, dependable synchronization is the primary reason HyperCube can achieve such high throughput. Traditional blockchains synchronize on large blocks of transactions. By synchronizing on blocks, a transaction cannot be processed until a period of time known as "block time" has elapsed. In Proof of Work consensus, these block times must be very long (at least 10 minutes) in order to reduce the chances of multiple validators producing a new valid block at the same time. There is no such constraint in Proof of Stake consensus, but a validator cannot determine the order of incoming blocks without reliable timestamps. The most common workaround is to append a wallclock timestamp to each block. The timestamp is only accurate within an hour or two due to clock drift and network latencies varying. To get around the workaround, these systems extend block times to ensure that the median timestamp on each block is always increasing.

HyperCube takes a completely different approach, which it refers to as Proof of Dedication, or PoD. Leader nodes "timestamp" blocks with cryptographic proofs



that a certain amount of time has passed since the previous proof. All of the data hashed into the proof must have happened before the proof was generated. The node then distributes the new block to validator nodes, which can verify the proofs. The blocks can arrive at validators in any order, and they can even be replayed years later. With such dependable synchronization guarantees, HyperCube can divide large blocks into smaller batches of transactions known as entries. Before any notion of block consensus, entries are streamed in realtime to validators.

Although HyperCube never sends a block, the term is used to describe the sequence of entries that validators vote on in order to achieve confirmation. In this way, the confirmation times of HyperCube can be compared to those of block-based systems. Block time is currently set to 800ms in the current implementation.

Under the hood, entries are streamed to validators as fast as a leader node can batch a set of valid transactions into an entry. Validators work on those entries for a long time before voting on their validity. Because the transactions are processed optimistically, there is no delay between the time the last entry is received and the time the node can vote. If consensus is not reached, a node simply rolls back its state. This optimization processing technique, known as Optimistic Concurrency Control, was introduced in 1981. It can be used in blockchain architecture, where a cluster votes on a hash that represents the entire ledger up to a certain block height. It is easily implemented in HyperCube by using the last entry's PoD hash.

## **POD and VDF**

HyperCube first described the Proof of Dedication technique for use in blockchain in November of 2017. In June of the following year, a similar technique known as a verifiable delay function, or VDF, was described at Stanford.

The fact that a VDF's verification time is very short is a desirable property. The approach taken by HyperCube to verifying its delay function is proportional to the time it took to create it. Split over a 4000 core GPU, it is fast enough for HyperCube's needs, but if you asked the authors of the paper cited above, they might (and have) told you that HyperCube's approach is algorithmically slow and shouldn't be called a VDF. We argue that the term VDF should refer to the entire category of verifiable delay functions, rather than just the subset with specific

performance characteristics. Until that issue is resolved, HyperCube will most likely continue to refer to its application-specific VDF as PoD.

Another distinction between PoD and VDFs is that a VDF is only used to track duration. PoD's hash chain, on the other hand, includes hashes of any data observed by the application. That information is a two-edged sword. On the one hand, the data "proves history," implying that the data existed prior to the hashes that followed it. On the other hand, it implies that the application can manipulate the hash chain by changing the time at which the data is hashed. As a result, the PoD chain does not serve as a good source of randomness, whereas a VDF without that data could. The leader rotation algorithm in HyperCube, for example, is derived solely from the VDF height and not its hash at that height.

## Storage

### Blockthread

A blockchain is formed when all consecutive blocks from a block that has reached finality, all the way back to the genesis block, unite to form a linear chain that is generally referred to as the blockchain. To keep the network running until then, the miner is responsible for maintaining all potentially viable chains, which are referred to as forks. Detailed explanation of the method by which forks spontaneously develop as a result of alpha node rotation may be found in the section on fork creation. A miner's ability to cope with forks until blocks are completed is facilitated by the use of the blockthread data structure described here.

Every shred a miner observes on the network, in any order, must be signed by the expected alpha node for that specific slot in order for the miner to record it. This is performed using the blockthread, which is used to ensure that every shred is recorded.

Fork-able key space relocation is accomplished by relocating shreds to an alpha node slot + shred index tuple. The tuple of alpha node slot + shred index represents the fork-able key space relocation (within the slot). The skip-list structure of the HyperCube protocol can be stored in its whole as a result of this, eliminating the need to determine which fork to follow, which Entries to persist, or when to persist them.

Blockthread's store implements this concept by serving current shred repair requests from RAM or recent files, whereas less recent shred repair requests are serviced from deeper storage, as demonstrated by the store that supports blockthread.

### Persistence

Located in the foreground of the node's verification process, immediately following network receive and signature verification is the Blockthread. Immediately after receiving a shred, if it is consistent with the alpha node schedule (i.e., if it was signed by the alpha node for the indicated slot), it is stored.

### Repair

Repair is the same as described above for windows, but it is capable of serving any shred that has been received. Blockthread stores shreds that have been signed, allowing the origination chain to be preserved.

## **Forks**

Due to the fact that Blockthread allows for random access to shreds, it can accommodate a miner's requirement to rollback and replay from a transaction processor checkpoint.

## **Restart**

The Blockthread can be replayed by ordering the enumeration of items from slot 0. This can be accomplished with suitable pruning/culling. Because of this, the logic of the replay stage (which includes dealing with forks) will have to be applied to the most recent entries in the Blockthread to ensure that they are correctly identified.

## Build

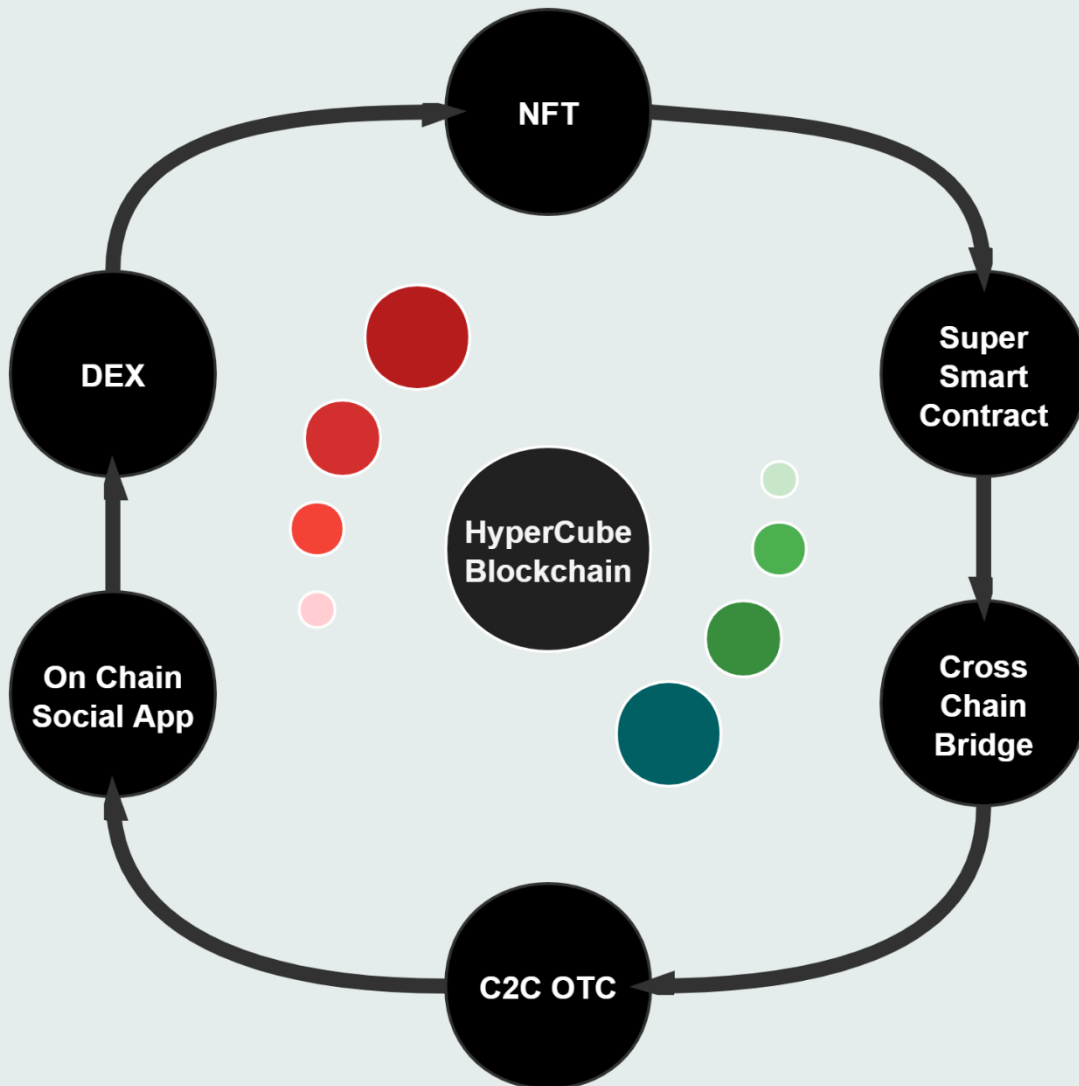


FIGURE 3 HYPERCUBE UTILITY

The following section will introduce key technologies of HyperVerse: XVM Virtual machine, XRC standard, XRexx language, MetaPlant, as well as some key use cases, like C2C, Social Network, and gameFi.

These tools and platforms are comprehensive, easy to use, modular, enabling developer and creator to create powerful and interesting DeFi, NFT product to realize SocialFi and GameFi on HyperCube.

Ethereum DApps and Smart Contract can transfer to HyperCube seamlessly, and the thus empowering the vast dev community on Ethereum.

HyperCube support Social DApp like on chain messenger, on chain facebook, with complete Decentralized Identifiers support, realizing the Anonymous Protection for Individual Information, and C2C online transaction, which lay the foundation of on chain commerce.

HyperVerse is the metaverse implementation platform on HyperCube, together with MetaPlant, HyperGame, users can create, share, trade, and interact NFT collectibles, provides an immersive experience in the metaverse crafted by HyperCube technology.

## XVM Virtual Machine

HyperCube Chain adds value to the ecosystem by allowing developers to create their own distributed apps using a wide range of tools. As illustrated in the diagram below, the HyperCube chain includes a Rexx-based programming language XRexx and a matching virtual machine XVM. Developers on the HyperCube Chain use programming languages to convert business logic into smart contracts, which are then converted into bytecodes that machines may run using virtual machines.

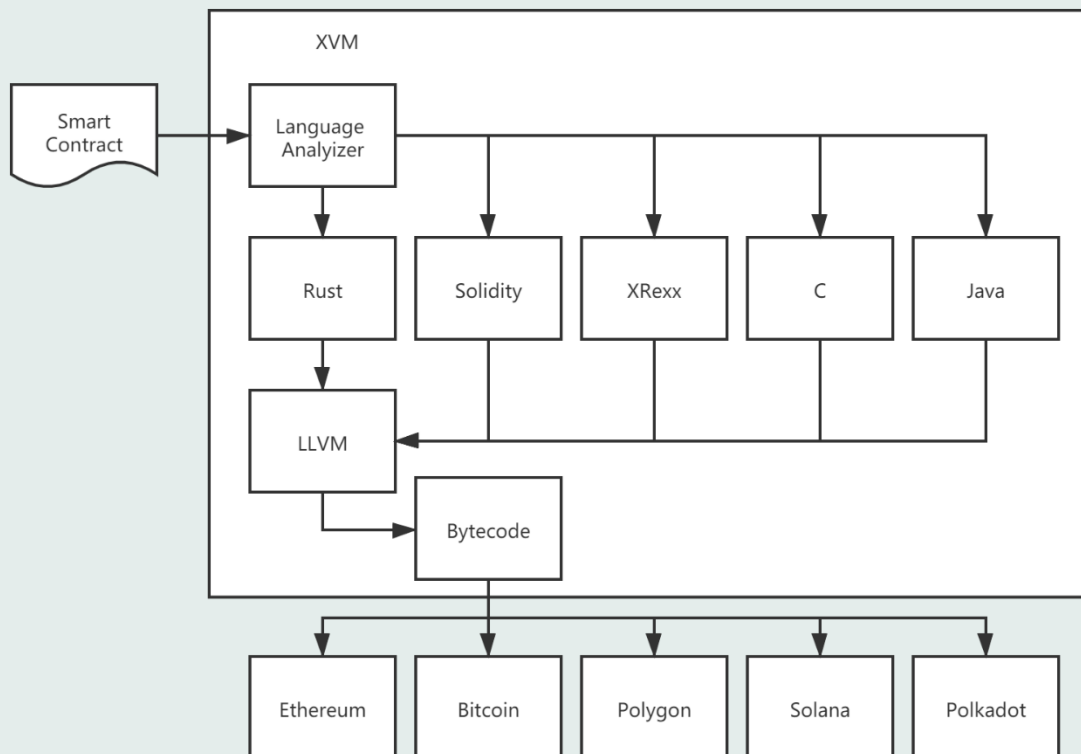


FIGURE 4 XVM ARCHITECTURE

## **XRC20 Standard**

One of the most important tools for doing business in HyperCube is the use of XRC20 currencies. A tokenization of some kind is represented by an XRC20 coin, which has coin sizes with melt values that are very tiny yet represent something else at a high ratio. (An XRC20 coin has a preset divisibility of one billion by default. The fact that a HyperCube is a trillion Mojo (which is the smallest indivisible unit, equivalent to a Satoshi in Bitcoin) means that there is space for such an operation. On the surface, this seems to be the same as the Omni protocol (a coloration format for Bitcoin), however the coloration of coins may be verified in a very simple and straightforward way. In fact, it is so lightweight that even smart coins may perform this function, as opposed to the Omni protocol, which needs operating a complete node in order to determine whether XRC20 coins are genuine. This is accomplished while maintaining the potential of XRC20 coins to perform at least as well as non-XRC20 coins in terms of intelligence. It is also possible to have one XRC20 currency incorporated in another XRC20 coin.

One of the additional pieces of functionality that our XRC20 currency implementation makes possible is the ability to make 'offers' to other users. Suppose you wish to exchange some HyperCube for some of an XRC20 currency. You might create an incomplete transaction in which some HyperCube is burned and some of the XRC20 coin is printed. The transaction itself will be void, but you may take your offer and submit it to an exchange, or send an email copy of it to a friend, or post it on Reddit. It will be possible for whoever receives it to accept the offer by creating their own partial transaction, which prints a counterbalancing amount of HyperCube and burns a counterbalancing amount of XRC20 coin, and combining it with yours to form a valid transaction that will be recorded on the blockchain. Considering that in HyperCube everything in a block occurs concurrently, the money are effectively transferred in a single step from one input to the other output, and there is never a point at which there are too many coins in the system. In reality, it is feasible for a third party to handle the bookkeeping of numerous offers involving a number of different assets, and as long as the totals line up, everything will go through as planned.

## **XRC77 Standard**

The following standard enables the creation of a standardized API for non-fungible tokens within smart contracts. This standard defines the fundamental functionality required to track and transfer NFTs.

We examined both private ownership and transaction of NFTs as well as consignment to third-party brokers/wallets/auctioneers ("operators"). Non-financial tokens (NFTs) can be used to represent ownership of digital or physical assets. We evaluated a wide variety of assets, and we're sure you'll think of many more:

Physical property – residences, one-of-a-kind artwork

Virtual collectibles – one-of-a-kind cat images, collectible cards

Assets with a "negative value" — loans, obligations, and other responsibilities

By and large, each house is unique, and no two kittens are same. NFTs are distinct from one another, and you must track their ownership separately.

## **XRC155 Standard**

### **Standard Mass Transfers**

The XRC155 standard enables the native transfer of large amounts of tokens from a smart contract to another smart contract. Using this method, we may transfer many NFT tokens or fungible tokens (or both) in a single operation, allowing us to complete the transfer in a single action. This is particularly useful if we have a series of NFT tokens or fungible tokens (or both). It is feasible to save money on transaction fees, reduce the effect on the network, and make it much easier to implement a trading system (escrow/atomic swap) utilizing the tokens in question.

### **Multiple Token Contracts**

An XRC155 may also explain the presence and functioning of several tokens at the same time, in addition to the above features. It may thus generate and describe one or more fungible tokens (such as the XRC155) while simultaneously describing one or more non-fungible tokens (such as the XRC77) inside the same contract, therefore simplifying the deployment and programming of the tokens.

### **Integrated Token Type Detection**

Another feature of the XRC155 token is the possibility to incorporate the functionality of the XRC165 token (also known as the Standard Detection Interface) into the same system as the XRC155 token. Thus, the XRC155 token is able to detect the interface of a token and modify its behavior in response to that interface's detection. This is particularly helpful owing to the fact that the XRC155 is a multitoken coin, and thus simplifies the design of applications.



## **Secure Token Transfer**

The safe token transfer function of the XRC155 token is maybe one of the most promising aspects of the token. In order to do this, the XRC155 standard smart contract contains a function that checks that the transaction has been completed and, if it has not, reverts the transaction to allow the tokens to be returned to their issuer. This is particularly helpful when we make a mistake in the transcription or copying of addresses and instead send our tokens to the incorrect address, rendering our transaction ineffective. In such scenario, the transfer is considered invalid, and the issuer recovers the tokens, enabling it to check the address once again and repeat the transaction if necessary. For the purpose of avoiding assaults from double spending, a number of rules have been defined that prohibit this behavior, keeping it secure against these kinds of attacks and other traps in general.

## **XRexx**

### **Introduction of XRexx**

HyperCube provides a solid support for DeFi Development. Additionally, as part of the HyperCube project, we've developed a new on-chain programming environment called XRexx, which is every bit as powerful as Solidity while also being much more auditable and scalable. Additionally, it promotes significantly improved software development methods.

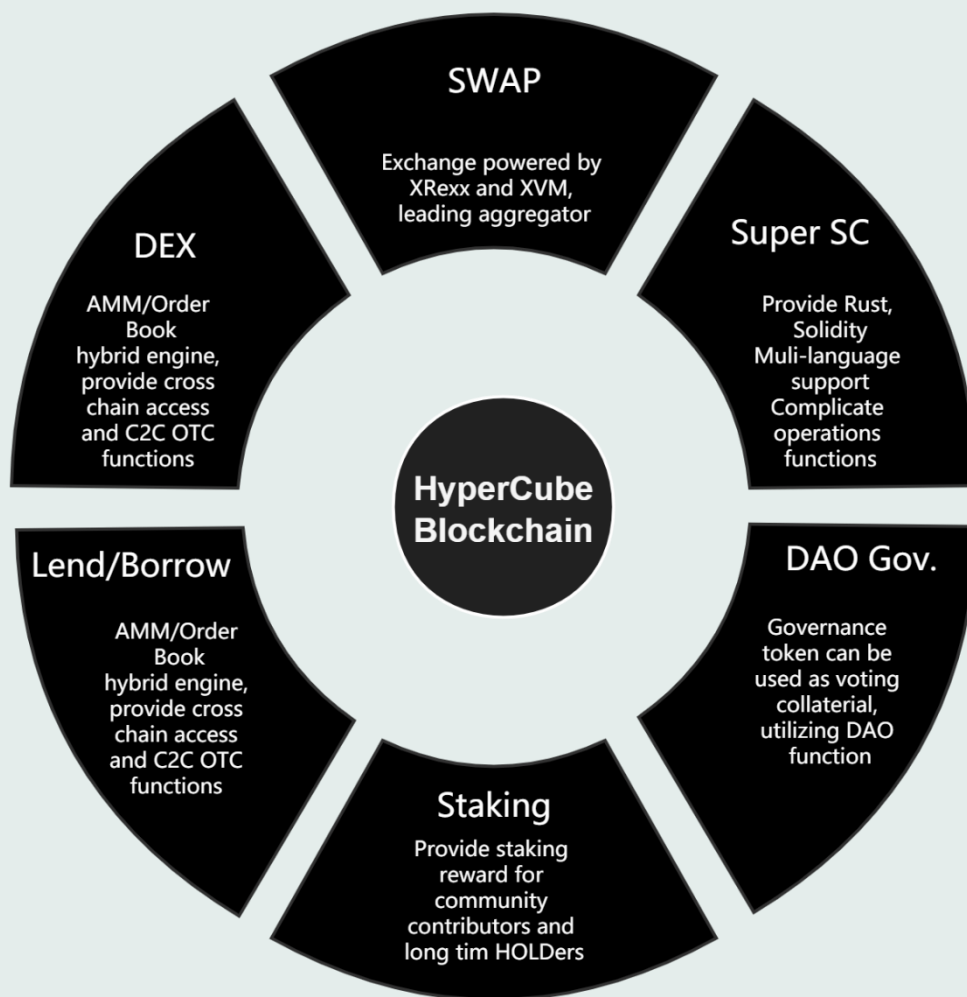


FIGURE 5 DEFI ON HYPERCUBE

As an illustration of the strength of on-chain programming in HyperCube, and how it varies from Solidity, I'll provide a summary of how it allows fully decentralized exchange while providing substantial protections against miner/farmer extracted value in this article (MEV). In addition, I will discuss the advantages of using automated market makers (AMMs) in HyperCube trading.

HyperCube operates on a coin set concept (which is comparable to Bitcoin's UTXO mechanism) as follows: The only thing that remains constant is the current set of unspent coins, which are distinguished by their sizes and the rules that govern how they may be spent. When a coin is spent, the value of the coin may be used to create new coins, but the value of the original coin is lost forever. All permanent data must be stored in the form of coins. This is significantly better for scalability since the data that full nodes have to keep track of is simpler and smaller than the objects that the EVM needs to store, and therefore far more efficient. Validating a

block requires the completion of all of its transactions, with the only output being a list of coins that have been spent and destroyed. Because of this, we are able to achieve an effective transaction rate that is higher than Ethereum's while still being able to operate a complete node on a typical desktop computer. At first glance, it seems that the flattening of data types will make it much more difficult to create smart coins in HyperCube, however the flattening of data types has many significant advantages. Everyone and everything communicates and cooperates with one another, and bits of functionality may be reused and layered on top of one another

## **Robust Analysis of XRexx**

XRexx is the smart contract language for HyperCube blockchain which enable DeFi programmability on chain.

We have recently released the first version of the XRexx programming language and on-chain programming environment, which offers a completely new and much improved method to developing smart transactions on the Ethereum blockchain. This article will provide an overview of the latest developments and how they are superior to previous models.

Up to this point, the two broad approaches to smart transaction environments that have emerged from Bitcoin and Ethereum have been referred to as 'the UTXO model' and 'the Solidity model,' respectively. As long as servers keep track of the current set of unspent coins (and their birthdates, which is a minor addition), transactions are only allowed to spend some coins and create others and are not allowed to rely on any external data, the only way for them to go from good to bad is for one of the inputs to be spent (or to be reorged into never existing or having a different birthdate, again a minor gotcha). While the Solidity model includes a large amount of on-chain information, including running applications, the consequences of a transaction cannot always be predicted before the transaction is executed. The UTXO method is much simpler, easier to implement, has reduced overhead on full nodes, and results in smart transactions that are significantly more reliable, secure, and succinct. The Solidity model is much more hazardous, costly, and unreliable than the other models, but it has significantly more expressive potential.

### **Message Construct of XRexx**

Our solution for Solidity (and the surrounding CLVM) is to retain the UTXO paradigm while also incorporating the broad capability of the Solidity programming language. This is accomplished via a series of straightforward cleanups that, although individually insignificant, build up to something very powerful:

Bitcoin is a first-class object in which coins are represented as a transaction id and an output number, while transactions in Ethereum are ephemeral justifications for destroying some coins and creating others. In contrast, transactions in Bitcoin are first-class objects in which coins (UTXOs) are represented as a transaction id and an output number.

A significant reduction in the complexity of the coin format (UTXOs). It consists only of the main input, the puzzle hash, and the amount.

Transactions take place in real time rather than in a sequential fashion.

Using BLS, which is a non-interactively aggregatable format, signatures are created, and aggregation is performed at every stage.

There are no negative consequences from the words used. In comparison to the existing taproot concept for Bitcoin, this enables delegation and partial delegation in a far more broad and powerful manner.

The return value of all puzzle (scriptpubkey in Bitcoin parlance) solutions (scriptsigs) expresses the needs of the solutions (scriptsigs).

The language has achieved the turing completion. Considering that execution is temporary, this adds much less complexity than most people believe. Solidity's complexity is caused by the complicated persistent state that exists in the system.

Because the language has the required primitives for calculating coin ids, and because coins are capable of asserting their own ids, it eliminates the need for quines and enables explicit self-reference.

Apart from language and environment extensions, there are several programmatic techniques that allow for much more functionality than you would expect:

It is possible to construct covenants by stating assertions about the puzzle hashes of outputs that are applicable recursively. This could theoretically be accomplished using Bitcoin Script, but it lacks adequate string mangling skills and the ability to do a 'check signature from stack,' which was the motivation for utilizing Bitcoin Script in this instance.

A capability may be achieved by employing backwards pointing covenants, which refer to ancestors rather than descendants in order to achieve the desired result.

Coins may interact with one another via the use of ephemeral coins, which are spent in the same transaction in which they are generated and are declared as inputs by the currency that is receiving the communication.

When a reveal is obtained in a solution, state may be stored in inaccessible portions of the code, which can then be retrieved by asserting the coin id, which is computed based on the puzzle hash, which is calculated in the puzzle.

These methods, when combined, allow for the creation of arbitrarily complicated functionality without the need for any additional opcodes. New functionality may be created and deployed in a matter of minutes.

As an example of what may be done with this technology, we are making accessible a number of reference smart transactions and the wallets that utilize them, including the following:

A wallet that can only transfer money to those who have been authorized to receive them.

A wallet that can only spend money at a predetermined pace, as well as the ability to make payments to it non-interactively, is described as follows: If the wallet software is capable of creating several funds-holding coins and spending from all of them at the same time, this seems to be required in order to do this.

It is similar to a paper wallet in that it contains deposit recovery information, but it has a reduced attack surface. It can be used to recover funds from a wallet whose secure hardware has failed; however, unlike a traditional paper wallet, instead of immediately gaining control of the coins, the deposit recovery information can be used to initiate a process for gaining control that takes some time, during which the hardware wallet (if it is still online) can claw the funds back from the deposit recovery information. Furthermore, it may support the need of a deposit to begin the healing process, which the person who has been assaulted has the ability to "take."

As well as this, we've created implementations of certain fundamental Bitcoin functionality that already exists but is important:

Multisig. We're beginning with the most basic method, which is the same as it is in Bitcoin, and will be implementing the more advanced ways, which make excellent use of signature aggregation, in the next months.

Swaps at the atomic level. We have a smart wallet that does the exchange and deals with all of the edge situations on the blockchain.

Further reference smart transactions will be developed in the future, and the XRexx feature will be implemented on our testnet before being rolled out to our mainnet. Prior to the final launch of the mainnet, there will be incompatible modifications, but the core principles will remain unchanged. In the coming months, we will be adding some interesting new reference transactions to this list, including light client

verifiable colored coins that inherit full XRexx capability, as well as distributed identity wallets with advanced recovery capabilities.

# Metaverse

HyperVerse is the extended reality crafted by the HyperCube platform.

## HyperVerse

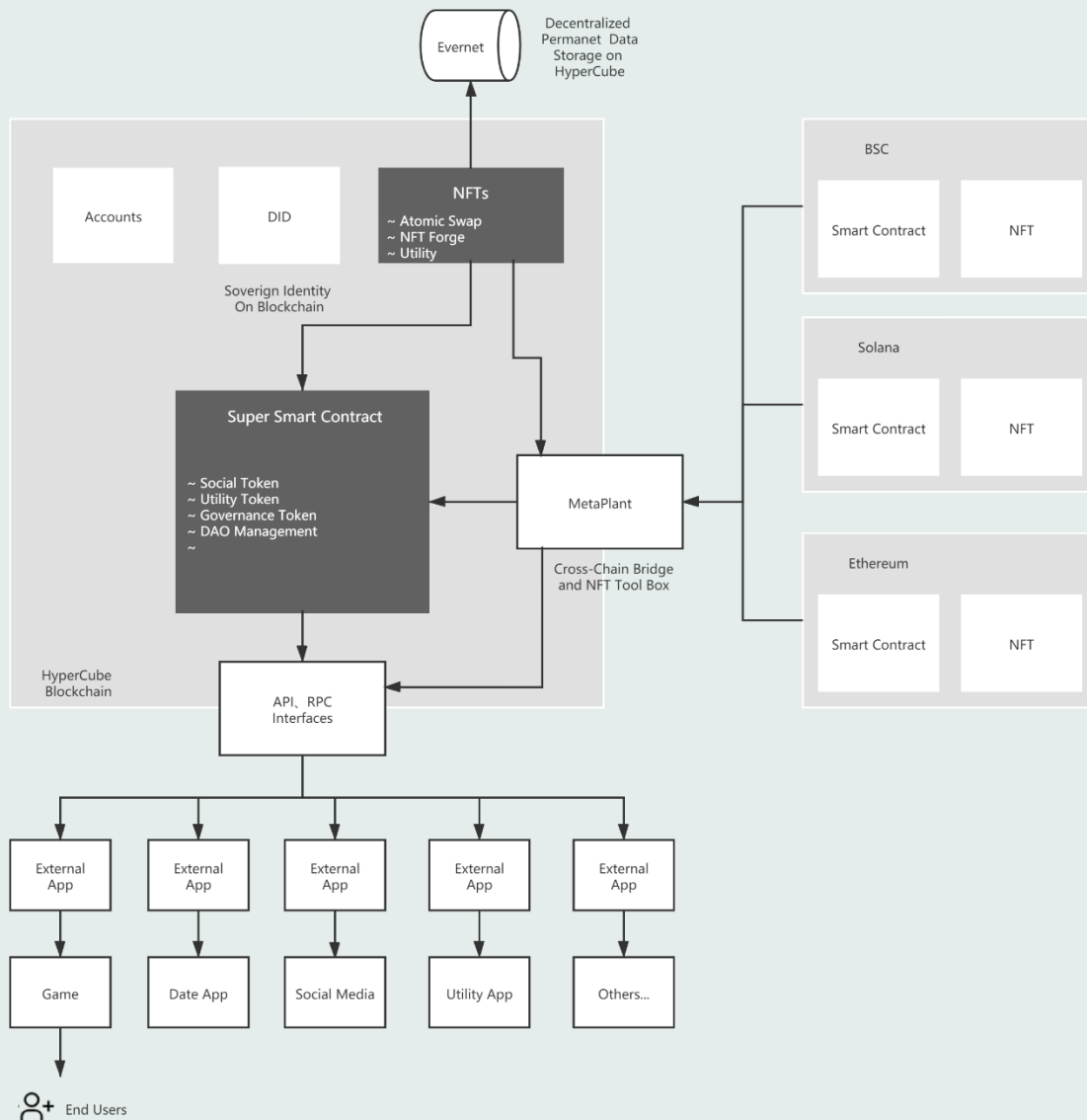


FIGURE 6 HYPERVERSE TECH ARCH

## The Metaverse Based on HyperCube

Consider the following scenario: you're strolling along the street. Suddenly, you come up with an idea for a product you need. A vending machine emerges immediately next to you, stocked with the product and variants you were

considering. Then you pull over, choose an item from a vending machine, have it delivered to your home, and continue on your way.

After that, visualize a husband and wife. The husband offers to take the wife to the shop, but she is unable to recall the product's name or the kind of goods she need. When she walks inside the shop, her brain-computer interface gadget identifies it and sends a connection to her husband's device, as well as the names of the stores and aisles where it is situated.

In the metaverse, alternative digital worlds exist where individuals work, play, and interact with one another. There are several names for this phenomenon, including the metaverse, the mirror world, the AR Cloud, the Magicverse, the Spatial internet, and Live Maps, but one thing is certain: it is on its way, and it is going to be huge.

If you Google the word "metaverse," you'll come up with a slew of definitions. According to Wikipedia, it is a collective virtual shared place that is produced by the convergence of virtually improved physical reality and physically persistent virtual space, which includes the total of all virtual worlds, augmented reality, and the Internet, among other things. The term "metaverse" is a portmanteau of the prefix "meta" (meaning beyond) and the word "universe." It is typically used to describe the concept of a future iteration of the internet that is made up of persistent, shared, 3D virtual spaces that are linked together to form a perceived virtual universe; the term "metaverse" is a portmanteau of the words "meta" (meaning beyond) and "universe."

You can now only experience the internet when you physically travel to it, but with new connections, gadgets, and technologies we will be able to experience it all around us, every single day of our lives.

If you are having difficulty picturing it, here is a concept film from Adobe as well as some of the finest examples of what it might look like. The video begins at the two-minute mark and continues to the end.

The metaverse, which is more than just a word from a Neal Stephenson science fiction book, is now being constructed. Kevin Kelly of Wired magazine published a cover article for the magazine in 2019 titled "Welcome to the Mirrorworld." In it, he explains how augmented reality will serve as the catalyst for the next major technological platform. In essence, "we are creating a one-to-one map with an almost inconceivable level of detail." When it's finished, our physical world will be seamlessly integrated with the digital universe." So prepare to meet your digital twin, as well as the digital twins of your home, nation, workplace and perhaps your whole life (if you want to participate).



So, what happens when the environment becomes a billboard, robots are capable of spatial thinking, and virtual assistants have complete control over the consumer's interaction with them? If this question caused you to stop for a split second, you should continue reading.

Currently, the metaverse is a shared virtual environment in which individuals are represented by computer-generated characters known as avatars (think Ready Player One). The virtual world is continuously expanding and evolving as a result of the choices and actions taken by the civilization that exists inside it. People will eventually be able to join the metaverse fully virtually (i.e., via virtual reality) or interact with portions of it in their physical environment through the use of augmented and mixed reality technologies.

At the VRARA Global Summit, Leslie Shannon, Nokia's Head of Trend Scouting, spoke about the significance of the metaverse, also known as the spatial internet, and how it will shape the future of technology. During her presentation, she said that "the spatial internet represents the conclusion of everything that is now being developed in the fields of AR and VR." Taking information about objects, places, or historical events and actually placing that information out in the world where it is most important is the concept of geolocation." This information layer will be visible via the use of augmented reality and virtual reality technologies.

Professionals in marketing and communications must pay close attention to the metaverse since it is the next frontier in online engagement. Just as social media has transformed the internet marketing environment, the metaverse is poised to do the same in the future. While we do not yet have a single common metaverse, there are businesses positioning themselves to work on establishing one in the near future.

Fortnite, Minecraft, and Animal Crossing are all now available as games, but they already have large user bases, complex environments, and a plethora of user-generated material. The virtual reality social media platform Horizon (which is presently in development) and Facebook Live Maps are both examples of how the social media giant is positioning itself towards the metaverse. Niantic, Magic Leap, Microsoft, and a slew of other companies are all working on it.

The epidemic has also had an impact on online culture. Organizing family reunions on Zoom, having marriages in Animal Crossing, having graduations in Minecraft, and digitally putting on clothing have all become popular activities. With online social gatherings growing more popular and online video games expanding their world-building capabilities, "it's inevitable that brands will play a major role in the metaverse," according to the authors.



## MetaPlant

### A Creation Platform on HyperCube

MetaPlant is a blockchain collaboration platform that connects artists, marketers, and developers, enabling them to create non-fungible tokens (NFT) that are increasingly useful in various projects. Meta provides a variety of complex functions.

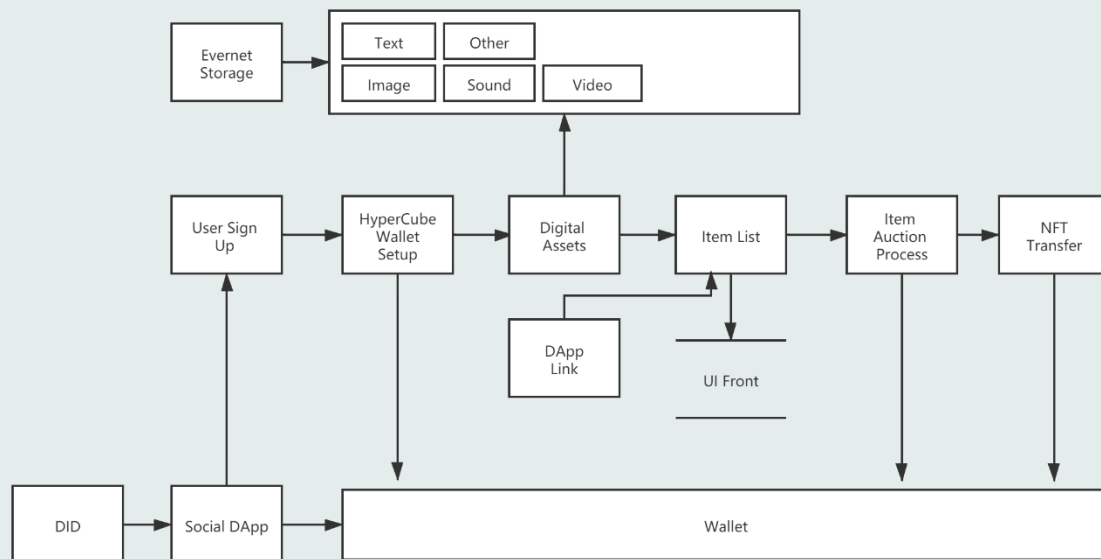


FIGURE 7 METAPLANT PROCESS

### DApp Link

MetaPlant is a unique network where NFT producers and utility providers come together to link content across distributed applications.

### NFT Browser/Market

Now, for the first time, artists, brands, and decentralized applications (dApps) can use the rapidly expanding cross-usable non-fungible token ecosystem to explore, collaborate, and create distributed asset networks.

### Collaboration Platform

MetaPlant is built as a network of linked projects, allowing everyone from artists and brands to game developers and application developers to collaborate on projects that can be accessed and used in multiple ways.

FIGURE 8 NFT CREATION PLATFORM

## Network Traffic Entrance

When using non-fungible tokens (NFT), there is virtually no limit to the number and types of utility items that can be unlocked in various worlds using non-fungible tokens. By combining with cooperative dApps, projects can leverage existing NFTs and communities, and users can find new games and applications to explore their NFT collections.

## NFT Extension

Because NFTs provide exclusivity as well as real digital ownership, they are the perfect medium for digital collectibles to be created. Many dApp, content producers, and artists have issued millions of NFTs to tie them to particular material and give them with transferrable ownership rights in exchange for their work.

On its own, this feature has the potential to fundamentally alter the way we value, consume, and transmit digital material in the future. The real superpower of NFTs, on the other hand, extends well beyond these characteristics and is found in their decentralized nature.

Currently, the vast majority of NFTs are of little or no use, and their services are often supplied by the same company that developed them in the first place. In the case of a dApp, access to content is given only when the user confirms ownership of the associated NFT via the use of a blockchain wallet (or similar mechanism).

Compared to traditional applications, where access is regulated via a centralized user account system, this is a significant difference.

It is in this area that NFTs have such tremendous, mostly unexplored potential:

Third-party dApps are able to provide permissionless extra services due to the fact that they are decentralized, user-owned, and publicly controlled. In addition, there is no restriction on the quantity or kind of utilities that NFTs may unleash across a wide range of domains, which is a very interesting element of this function.

This opens up hitherto unimaginable opportunities for the integration of digital goods and services into cooperative networks (as initially envisioned and described in the HyperCube Multiverse).

Because they are interacting with existing NFTs and communities, projects may become part of collaborative dApp ecosystems and attract new users by offering additional utilities and expanded use-cases while also contributing value to the underlying network of nodes.

In contrast, users may explore the utilities of their NFTs, remain up to date, and get notifications if new utilities are introduced to their assets.

## **DApp Link**

Projects may use MetaPlant to build, examine, and link NFT Blueprints and Utilities across a variety of dApp.

Those who create NFTs (such as decentralized applications (dApp), businesses (such as brands), artists (such as content creators), streamers (such as celebrities), and others can use the platform to integrate third-party utility into their tokens, allowing their holders to benefit from additional use-cases.

Similarly, utility providers (e.g., video games, services, platforms, events, and online shops) may provide utilities for particular NFT blueprints in order to benefit and attract the holders of these blueprints.

These connections are established as a result of cooperation requests made between projects in order to create a new link within an ever-expanding network of assets.

Request for collaboration between two projects in order to connect an NFT to a utility The scope of the collaboration may be tailored by adding restrictions and quotas to the cooperation request when it is sent in order to connect with a specific asset. This enables for the creation of limitless or temporary utilities that may be either consumable (e.g., vouchers, mana, event tickets, coupons) or non-consumable (e.g., coupons, event tickets, coupons) (e.g., memberships, virtual characters).

Holders of NFTs will be informed when a link has been made and will be given access to the newly created utility once it has been established.

## **Social DApp**

QuantumChat is an in-house instant messenger developed by HyperCube. It is a dApp (decentralized application) built on the HyperCube network using the Athena SDK.

QuantumChat protects all of your personal information completely through the use of Decentralized Identifiers. The blockchain-based network intends to be a global platform for free, anonymous, and secure communication, enabling users to conduct private chats via phone or text messaging.

Rather than keeping data on a centralized server, which is the most popular means of relaying communication data today, QuantumChat protects users' privacy by

transporting and distributing messages via decentralized file sharing via HyperCube blockchain technology.

By utilizing the aforementioned distribution techniques, the software ensures ultimate anonymity for its users while also safeguarding their encrypted data, making it impregnable to hackers and malicious attacks of any kind.

Additionally, the QuantumChat application does not gather users' personal information, as just a username and password are necessary for app registration and access to users' individually stored, protected data on the QuantumChat app blockchain.

The QuantumChat app, which is presently in development, was developed with a billion-user audience in mind by the QuantumChat team. Each user of the QuantumChat app will be assigned a unique DID. Additionally, users will have the option of storing their texts on their phone and deleting them at any moment.

QuantumChat is a versatile application that may be used for a variety of purposes, including messaging, on-chain trade, and other services.

## **Conclusion**

We've described how to create a multi-chain network with scalability and nonlinearity, with backward compatibility, and extension capability to be a creation platform or an underlying infrastructure in various use cases.

Within this system, participants work with the interests of themselves and the community in mind, since it's not just beneficial to the group as a whole, but to the individuals as well.

That's because the system can grow without users having to bear any of the additional expense usually associated with a blockchain design. A framework for the approach we are taking has been set with an overview of how it would look and feel. We describe the participants, their motivations, and how the whole process would work. We've pinpointed an effective general design, analyzed its advantages and shortcomings, and therefore have clear new objectives that we believe will make the design more robust and ultimately allow us to achieve our goal of developing a completely scalable blockchain system.

## **Reference**

[1] F. Tschorsch and B. Scheuermann, "Bitcoin and beyond: A technical

survey on decentralized digital currencies," IEEE Communications Surveys Tutorials, vol. 18, no. 3, pp. 2084–2123, thirdquarter 2016.

[2] M. D. Pierro, "What is the blockchain?" Computing in Science Engineering, vol. 19, no. 5, pp. 92–95, 2017.

[3] S. Nakamoto, "Bitcoin: A peer-to-peer electronic cash system," Tech. Rep., 2008. [Online]. Available: <https://bitcoin.org/bitcoin.pdf>

[4] G. Wood, "Ethereum: A secure decentralised generalised transaction ledger," Ethereum Project Yellow Paper, vol. 151, pp. 1–32, 2014.

[5] M. E. Peck, "Blockchain world - do you need a blockchain? this chart will tell you if the technology can solve your problem," IEEE Spectrum, vol. 54, no. 10, pp. 38–60, October 2017.

[6] D. T. T. Anh, M. Zhang, B. C. Ooi, and G. Chen, "Untangling blockchain: A data processing view of blockchain systems," IEEE Transactions on Knowledge and Data Engineering, vol. PP, no. 99, pp. 1–1, 2018.

[7] T. Aste, P. Tasca, and T. D. Matteo, "Blockchain technologies: The foreseeable impact on society and industry," Computer, vol. 50, no. 9, pp. 18–28, 2017.

[8] S. Underwood, "Blockchain beyond bitcoin," Commun. ACM, vol. 59, no. 11, pp. 15–17, Oct. 2016. [Online]. Available: <http://doi.acm.org/10.1145/2994581>

[9] J. Yli-Huumo, D. Ko, S. Choi, S. Park, and K. Smolander, "Where is current research on blockchain technology? a systematic review," PLOS ONE, vol. 11, no. 10, pp. 1–27, 10 2016.

[10] M. Nofer, P. Gomber, O. Hinz, and D. Schiereck, "Blockchain," Business & Information Systems Engineering, vol. 59, no. 3, pp. 183–187, Jun 2017. [Online]. Available: <https://doi.org/10.1007/s12599-017-0467-3>

[11] T.-T. Kuo, H.-E. Kim, and L. Ohno-Machado, "Blockchain distributed ledger technologies for biomedical and health care applications,"

Journal of the American Medical Informatics Association, vol. 24, no. 6, pp. 1211–1220, 2017. [Online]. Available: <http://dx.doi.org/10.1093/jamia/ocx068>

[12] H. Shafagh, L. Burkhalter, A. Hithnawi, and S. Duquennoy, "Towards blockchain-based auditable storage and sharing of iot data," in Proceedings of the 2017 on Cloud Computing Security Workshop, ser. CCSW '17. New York, NY, USA: ACM, 2017, pp. 45–50.

[13] W. Matthews and L. Cottrell, "The pinger project: active internet performance monitoring for the henp community," IEEE Communications Magazine, vol. 38, no. 5, pp. 130–136, May 2000.

[14] S. Ali, G. Wang, and R. L. Cottrell, "Internet Performance Analysis of South Asian Countries using End-to-end Internet Performance Measurements," in 16th IEEE International Conference on Ubiquitous Computing and Communications (IUCC 2017), Guangzhou, China, 2017, pp. 1–8.

[15] S. Ines, J. Ubacht, and M. Janssen, "Blockchain in government: Benefits and implications of distributed ledger technology for information sharing," Government Information Quarterly, vol. 34, no. 3, pp. 355 – 364, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0740624X17303155>

[16] N. Z. Aitzhan and D. Svetinovic, "Security and privacy in decentralized energy trading through multi-signatures, blockchain and anonymous messaging streams," IEEE Transactions on Dependable and Secure Computing, vol. PP, no. 99, pp. 1–1, 2016.

[17] N. Szabo, "Formalizing and securing relationships on public networks," First Monday, vol. 2, no. 9, 1997. [Online]. Available: <http://ojphi.org/ojs/index.php/fm/article/view/548>

[18] K. Christidis and M. Devetsikiotis, "Blockchains and smart contracts for the internet of things," IEEE Access, vol. 4, pp. 2292–2303, 2016.



- [19] V. Gramoli, "From blockchain consensus back to byzantine consensus," *Future Generation Computer Systems*, 2017. [Online]. Available: <http://www.sciencedirect.com/science/article/pii/S0167739X17320095>
- [20] D. Kraft, "Difficulty control for blockchain-based consensus systems," *Peer-to-Peer Networking and Applications*, vol. 9, no. 2, pp. 397–413, Mar 2016.
- [21] T. Barbosa, R. Souza, S. Cruz, M. Campos, and R. Les Cottrell, "Applying data warehousing and big data techniques to analyze internet performance," in *2015 NETAPPS 4th Int. Conf. on Internet Applications, Protocols and Services*, 2015, pp. 31–36.
- [22] S. Wilkinson, J. Lowry, and T. Boshevski, "Metadisk a blockchain-based decentralized file storage application," *Tech. Rep.*, 2014.
- [23] G. Zyskind, O. Nathan, and A. Pentland, "Enigma: Decentralized computation platform with guaranteed privacy," *CoRR*, vol. abs/1506.03471, 2015. [Online]. Available: <http://arxiv.org/abs/1506.03471>
- [24] R. C. Merkle, "Protocols for public key cryptosystems," in *1980 IEEE Symposium on Security and Privacy*, April 1980, pp. 122–122.
- [25] S. Ratnasamy, P. Francis, M. Handley, R. Karp, and S. Shenker, "A scalable content-addressable network," *SIGCOMM Comput. Commun. Rev.*, vol. 31, no. 4, pp. 161–172, Aug. 2001.
- [26] A. Roehrs, C. A. da Costa, and R. da Rosa Righi, "Omniphr: A distributed architecture model to integrate personal health records," *Journal of Biomedical Informatics*, vol. 71, pp. 70 – 81, 2017.
- [27] P. Maymounkov and D. Mazieres, "Kademlia: A peer-to-peer information system based on the xor metric," in *Peer-to-Peer Systems*, P. Druschel, F. Kaashoek, and A. Rowstron, Eds. Berlin, Heidelberg: Springer Berlin Heidelberg, 2002, pp. 53–65.
- [28] M. Castro and B. Liskov, "Practical byzantine fault tolerance and proactive recovery," *ACM Trans. Comput. Syst.*, vol. 20, no. 4, pp.

398–461, Nov. 2002. [Online]. Available: <http://doi.acm.org/10.1145/571637.571640>

[29] J. Benet, “IpfS-content addressed, versioned, p2p file system,” arXiv preprint arXiv:1407.3561, 2014.

[30] M. Vukolic, “Rethinking permissioned blockchains,” in ‘ Proceedings of the ACM Workshop on Blockchain, Cryptocurrencies and Contracts, ser. BCC ’17, 2017, pp. 3–7. [Online]. Available: <http://doi.acm.org/10.1145/3055518.3055526>