# Chain

Whitepaper

# Table of Contents

**Chain**

# Disclaimer

**Chain**

Chain Token ("XCN") was issued and distributed by Chain, a corporation located in Saint Kitts and Nevis, and is bound by the arbitration agreement located on Chain.com/legal. XCN tokens are not securities, investments, or investment contracts, nor should they be construed as such. Instead, XCN tokens are a means of accessing discounts on Sequence, Chain Cloud, paying for invoices, accessing premium services, and voting for community-based programs. Materials published by Chain do not constitute the provision of advisory services regarding investment, tax, legal, financial, accounting, consulting, securities offering, or any other related services, nor are they recommendations to buy, sell or purchase any product or service. Further, materials published by Chain reflect the information available at the time of publishing and are subject to change without notice. DO NOT purchase XCN for any speculative purposes and only purchase units of XCN that you intend to utilize and consume on the Chain ecosystem. Chain will not be liable for any direct or consequential loss arising from the use of this material or its contents.

## About Chain

Chain is a cloud blockchain infrastructure solution that enables organizations to build better financial services from the ground up. Founded in 2014, Chain has raised over $40 million in funding from Khosla Ventures, Pantera Capital, Capital One, Citigroup, Fiserv, Nasdaq, Orange, and Visa. Chain has previously partnered and worked to build blockchain networks for Visa, Nasdaq, State Street, Citibank, and more.

Adam Ludwin was the founder of Chain. He earned his Bachelor's degree from UC Berkeley and an MBA from Harvard Business School. Ludwin began his career as a consultant with The Boston Consulting Group and then worked in the venture capital space, specializing in "Fintech" organizations at RRE Ventures. He was credited with investments in prominent companies, including Vine, Slack, Kik, and Paperless Post.

In 2018, Chain was acquired by Lightyear Corp., the commercial arm of the Stellar Development Foundation, the organization behind the Lumens cryptocurrency, which formed Interstellar. The price of the acquisition was not disclosed, but Forbes claimed that it was the equivalent of $500 million paid in Lumens.

In 2020, Chain was re-acquired to continue its mission to build a more robust global financial system through blockchain cloud technology. Chain is now operating as a privately held corporation with a newly established board of directors, officers and shareholders.

## Problems

Chain has identified two core problems in the financial and blockchain industry that it aims to tackle through its ecosystem of products: Legacy Financial Systems & Public Blockchain Infrastructure.

## Legacy Financial Systems

In the modern financial system, assets such as currencies, securities, and derivatives are typically held and traded electronically. This miraculous abstraction hides the true complexity of the system: a messy decentralized web of mutual obligations, indirect ownership, and periodic settlement. Transferring assets often requires point-to-point interaction between multiple intermediaries and the reconciliation of duplicated ledgers.

**This system has many downsides:**

- **Time:**　　　　　Settlement of asset transfers or payments often takes days.

- **Cost:**　　　　　Transfers involve fee payments to multiple intermediaries, and reconciliation has a costly overhead.

- **Transparency:**　It may be challenging to find out the status of a pending transfer or the current owner of an asset.

- **Atomicity:**　　Transfers may not be complete, and it is difficult to make one transfer conditional on another.

- **Security:**　　　The complexity of the existing system makes it difficult to prevent fraud or theft.

- **Finality:**　　　Whether transactions are reversible depends on the transfer mechanism rather than the business requirements of the transacting party.

Many of these problems could be addressed if asset ownership were recorded on a single shared ledger. But a combination of practical and technological constraints has made such ledgers difficult to adopt. Such a shared ledger would tend to require trust in a single party. That party would need to have the technical capacity to process every transaction in real-time. Additionally, to support reversible, atomic, or complex transactions, the ledger would need to support more sophisticated logic than simple ownership changes.

## Public Blockchain Infrastructure

Public blockchain networks operate in a decentralized manner based on peer-to-peer distributed ledger technology. This architecture allows data and transactions to be stored globally on tens of thousands of servers, with everything being public and transparent.

Running a node for a public blockchain network is time-consuming, requires expensive resources, and is time-consuming to maintain. Nodes are typically updated regularly, with upgrades coming at times weeks apart, requiring rebuilding an entire node or upgrading a client. In addition, blockchain nodes are new, and most public networks are only a few years old, so they are not designed with reliability in mind.

Certain transactions may involve analyzing millions of transactions and blocks, which may often time out and crash a node. This causes developers to keep a close eye on these nodes to monitor their health and uptime. At times, nodes may fall behind the network for various reasons, such as peering, issues with the internal state, and soft-forking on outdated branches. If these issues occur, it will impact those users, and you will be providing outdated and stale data without realizing the impact it can have on user experience.

Node management is complex and requires significant developer and hosting resources to maintain properly. These types of problems can be easily solved by implementing a SaaS model product that addresses the complexity of node operations and management. This will free up resources for developers and cut costs so that the client can focus on their own product and customer experience.

## Web3 Strategy

The term Web3 was created by Gavin Wood, the co-founder of Ethereum and the founder of Polkadot. Web3 is the next evolution of the internet designed to give control of web applications back to the users instead of owners and run on public blockchain networks.

The growing dominance of cryptocurrencies and blockchain has facilitated the rise of Web3 powered by decentralized networks. Designed to restore power to users and creators, this transformative internet movement is beckoning a paradigm shift in how we use the internet. Web3 solves this dilemma, giving back content creators complete control over their content. Harnessing the power of blockchain and cryptocurrencies, Web3 allows creators to tap into numerous monetization opportunities while simultaneously rewarding users for continued participation and patronage. This creates a circular economy free from the restraints of centralized platforms and intermediaries.

Chain's Web3 strategy is designed to unlock the capabilities of public blockchain networks and smart contracts at the infrastructure level through Chain Cloud. This capability empowers developers to focus on their application and users, dedicating fewer resources to maintain the nodes running their application.
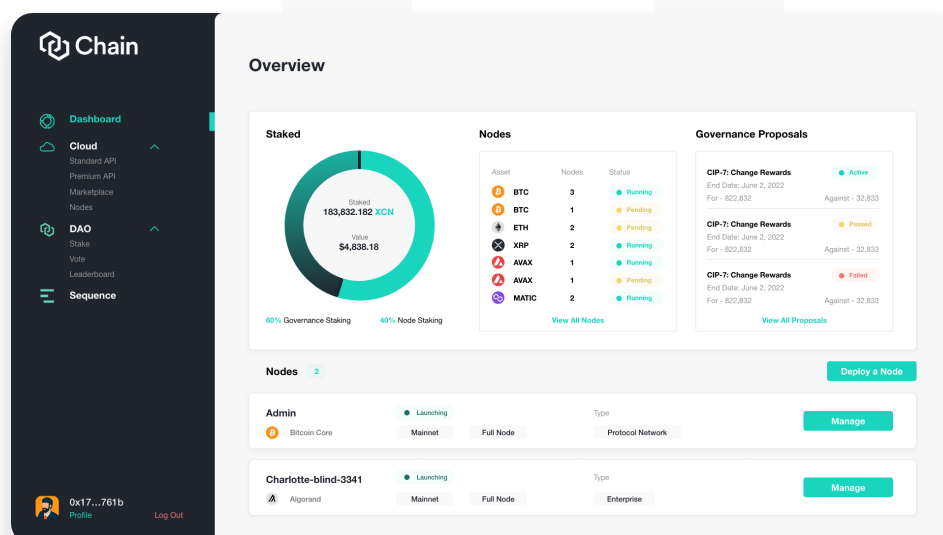
## Permissioned Architecture

Financial institutions and financial services providers who want to upgrade their legacy architecture with blockchain technology cannot assume the risks associated with public networks. A closed-ended blockchain will update antiquated technology while supporting both their compliance goals and their customers' needs.

Permissioned blockchains strike a balance between the benefits and security concerns around blockchain. A permissioned blockchain mitigates public blockchains' data privacy and security challenges by restricting participation in the blockchain to approved parties. To join the network of computers that can validate transactions on a permissioned blockchain, you have to have the approval of other members of the network.

Because permissioned blockchains provide decentralized transaction records without the privacy and security challenges posed by public blockchains, permissioned blockchains will help companies that want to store data on the blockchain without exposing it to the entire world. This creates a real-time settlement network for any type of asset, security, stock, or balance related item globally, digitally, and securely.

Chain addresses the needs of the permissioned blockchain space by giving companies the tools they need to deploy a private ledger with seamless development using Sequence.
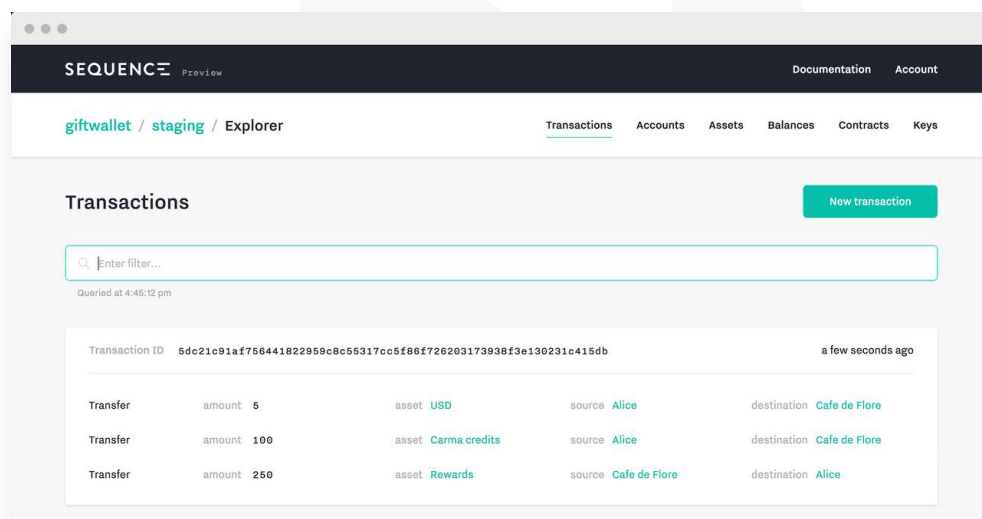
**Chain**

# Cloud

Chain Cloud is a decentralized and distributed infrastructure protocol designed for developers to access blockchain networks on-demand. In addition, clients can utilize various services within Chain Cloud to meet their blockchain and web3 product needs.

## Standard RPC / API

Chain's mission in building on our Web3 strategy begins with its free Standard RPC API for several public blockchain networks.

The Chain Cloud Standard RPC API is designed to give accessibility to a number of public networks to the community for free. This service enables reliable and fast API endpoints for developers globally to build on existing public blockchains.

Features:

- Free RPC API endpoints
- Open Network and permissionless
- Flexible limits
- Developer Dashboard
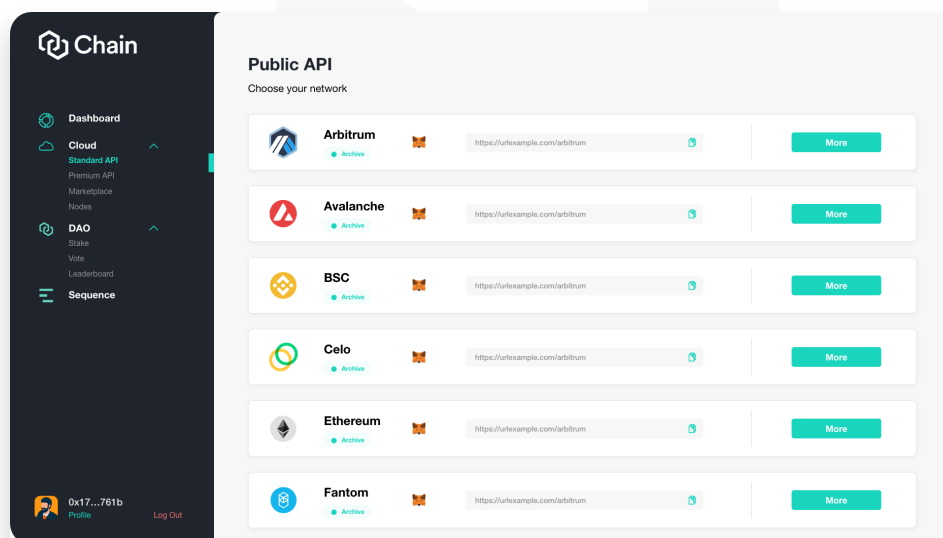
Chain Cloud's RPC layer is based on a globally distributed network of nodes and participants, creating a fully decentralized RPC API designed with fail-safe architecture. The underlying technology operates on multiple nodes across several data centers and home networks.

The protocol utilizes an internet monitoring system to ensure that the architecture is highly available and scalable. This ensures that all RPC API endpoints are constantly in sync with the underlying nodes. Chain Protocol routes the network traffic to ensure optimized routing and speed are available for developers.

## Premium RPC / API

Chain Cloud's Premium RPC API enables developers access to a wide range of extended services to build their project or application on an ultra-fast, secure and private network. Premium requires a fixed amount of XCN tokens paid annually, as defined by Chain Governance.

Features:

- Private & Secure Endpoints
- Low latency
- Advanced API endpoints
- Real-time analytics
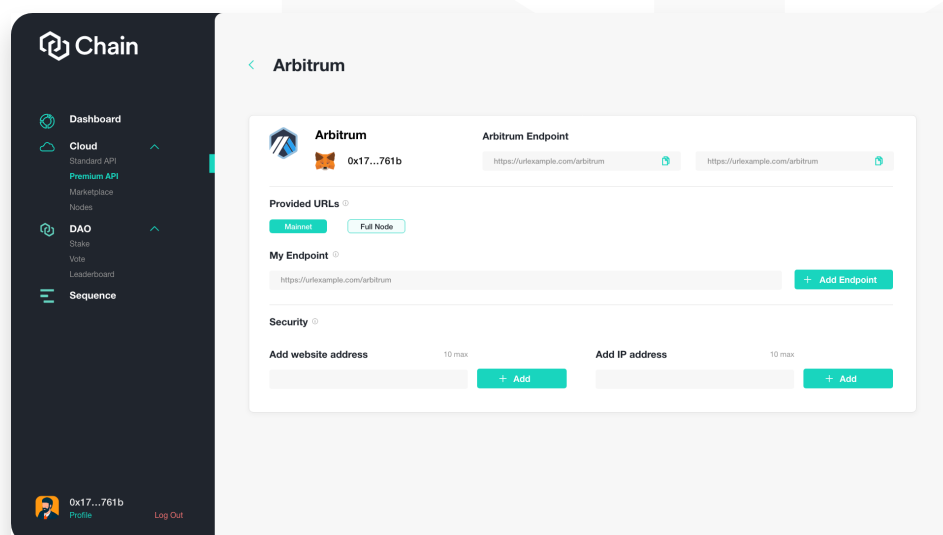
## Marketplace

Chain Cloud Nodes are a multi-cloud, multi-geo infrastructure platform for blockchain nodes, and we bring this capability to each network we support. Clients can deploy their node in any supported region globally through the interactive dashboard. Chain Cloud utilizes multiple cloud platforms and bare metal providers across many geographic regions and networks.
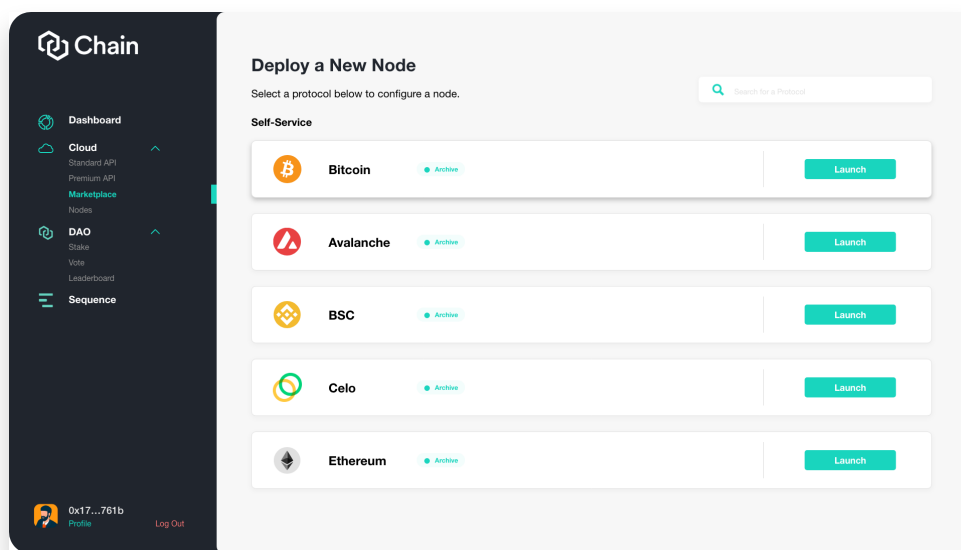


Nodes are constantly monitored through comprehensive tools. These data points and metrics are measured so that clients can view bandwidth, memory, disk space, and CPU load-on-demand. These alerting modules are working in real-time so that the platform can auto-scale when necessary to prevent any errors before their occurrence, including block heights, to ensure nodes are constantly in sync with the public networks.

Chain Cloud nodes exclusively belong to the client to run enterprise services or connect to the Chain Protocol. Clients enjoy the benefit of a dedicated node without the complexity of server management. Each node has a unique address, and its own set of authentication keys.

When protocol updates are developed and implemented, the updates demonstrate no disruption visible to the customer. Maintenance or upgrades to your nodes is automated based on node monitoring to constantly uphold the highest standards of network health, which you can track on demand with monitoring reports.

![Chain logo]

## Protocol Nodes

Chain Cloud Protocol Nodes are dedicated nodes deployed through the marketplace for developers that connect to the Chain Protocol. These nodes require XCN to be staked and bonded to the network in order to connect to the protocol. Once these nodes are connected, users are able to mine XCN rewards for providing their computing resources for the Chain Standard RPC API. These rewards and XCN requirements are determined by the Chain Governance on-chain proposals.
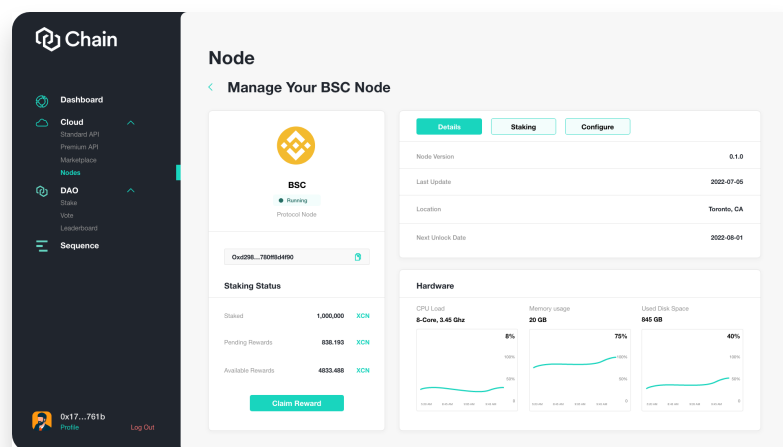


## Enterprise Nodes

Chain Cloud Enterprise Nodes are also fully dedicated nodes deployed through the marketplace and do not connect to any external protocol nor require staked XCN. Enterprise nodes are designed to be accessed only by the developer for their individual project(s). Developers can build robust and scalable web3 and blockchain applications to run their product without any DevOps development. Enterprise nodes can also be used to stake and delegate native tokens in their respective networks.
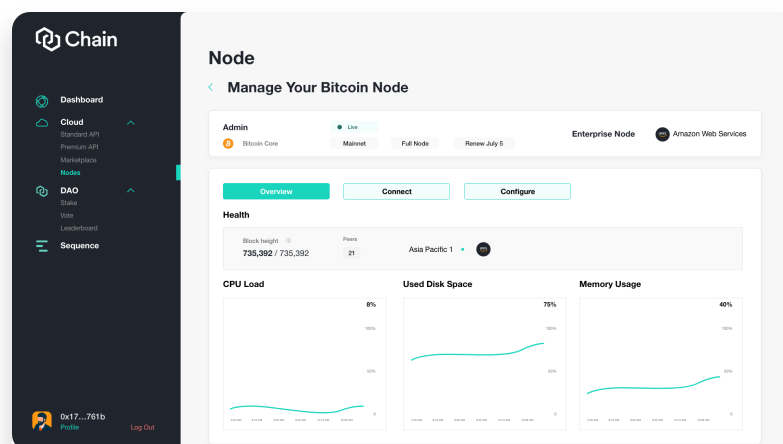
## Ledger-as-a-Service

Sequence is a cryptographically-secured cloud blockchain ledger service. It allows users to manage balances in financial and commerce applications like wallet apps, lending platforms, marketplaces, exchanges, and more. While ledgers are managed as a service, all transactions must be signed by the relevant keys. These keys are held in secure enclaves and controlled by the users, services, or organizations that have authority over particular assets, accounts, and functionality. Sequence cannot access them. This "cloud + keys" model is how Sequence combines tamper proof security with a great developer and operator experience.



Sequence lets modern software teams focus on shipping and scaling their product instead of building and maintaining ledger infrastructure. It does this by combining the convenience of a SaaS model with the security of cryptographic transaction signing. Under the hood, each Sequence ledger is an immutable, append-only data structure. Balances are represented by token-like objects called assets. Assets can be created, transferred, retired, or entered into more complex programs. A single transaction can include multiple actions involving any number of assets and accounts to ensure atomicity.

Sequence makes it easy to build, operate, and scale forward-thinking software products that need a secure and extensible system of record or smart contract application at their core.

Features:

- Secure Blockchain Ledger
- Export clean analytics and generate customized reports for different groups inside, and outside, your organization
- Easily add new transaction flows, balance types, and entities to the ledger
- Add custom applications through smart contracts

## Standard Plan

The Standard Plan gives developers the freedom to start building their applications on Sequence without any costs for up to 500,000 transactions per month.

Features:

- **Free**
- **Unlimited team members**
- **Unlimited accounts**
- **Unlimited queries**
- **Standard support**

## Premium Plan

The Premium Plan enables developers to build their application on Sequence with scalability on-demand and no restraints.

Features:

- **Unlimited team members**
- **Unlimited accounts**
- **Unlimited queries**
- **Unlimited transactions/month**
- **Dedicated 24/7 support**
- **Enterprise SLAs**

## Explorer

A Sequence ledger can be deployed by registering your team, creating a ledger, and embedding the Sequence SDK in the specified application. Development enclaves are provided so you can begin building immediately. There is also an easy-to-use dashboard where developers can prototype and query without writing any code.
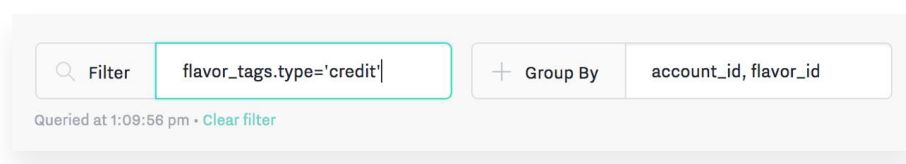
Sequence Explorer is a tool designed for developers and product managers. It enables both read and write access to the ledger (dependent on a person's role) through a convenient web interface. The explorer is helpful for prototyping your model, setting up your ledger, and debugging your application.
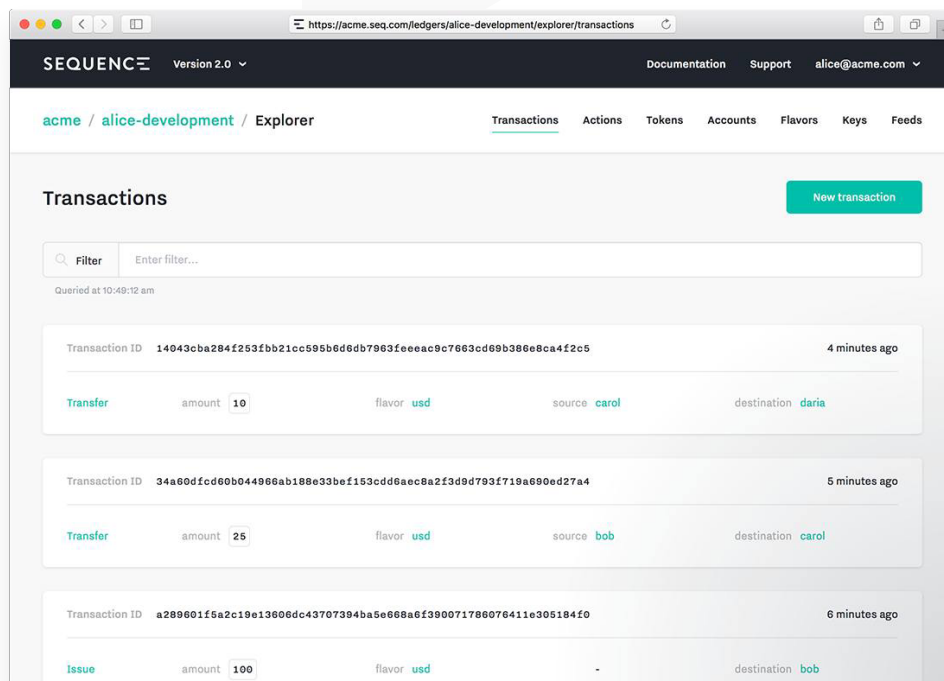
## Prototyping

As you are designing your ledger model, you can prototype all the interactions in the explorer without writing any code.

For example, you may wish to experiment with different asset tag configurations and the balance queries you can perform as a result. Explorer makes this task simple.
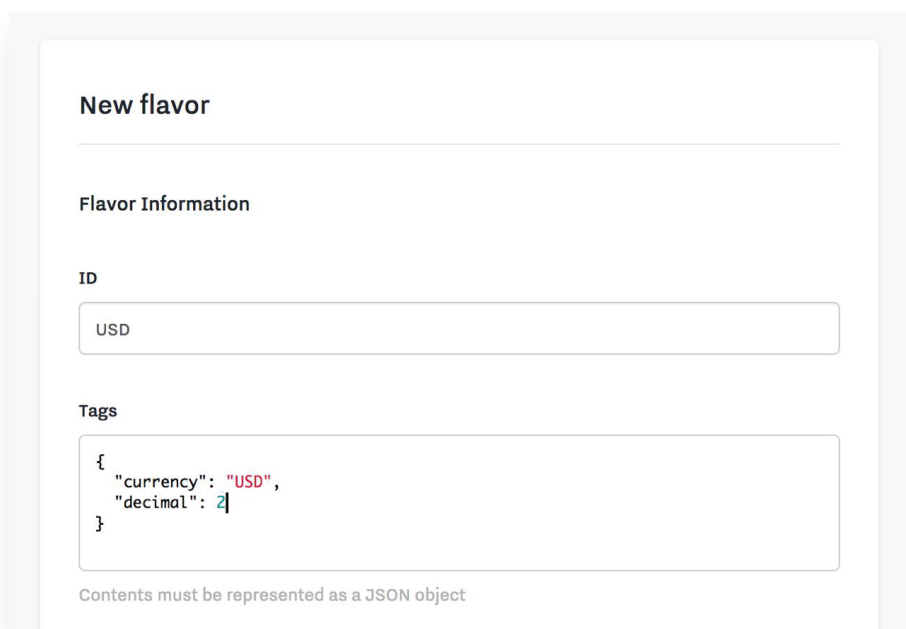


## Setup

Explorer is a great place to set up your application by performing operations that only need to occur once.

For example, if your application needs a fixed number of assets or accounts, you can create them in Explorer without writing any code.
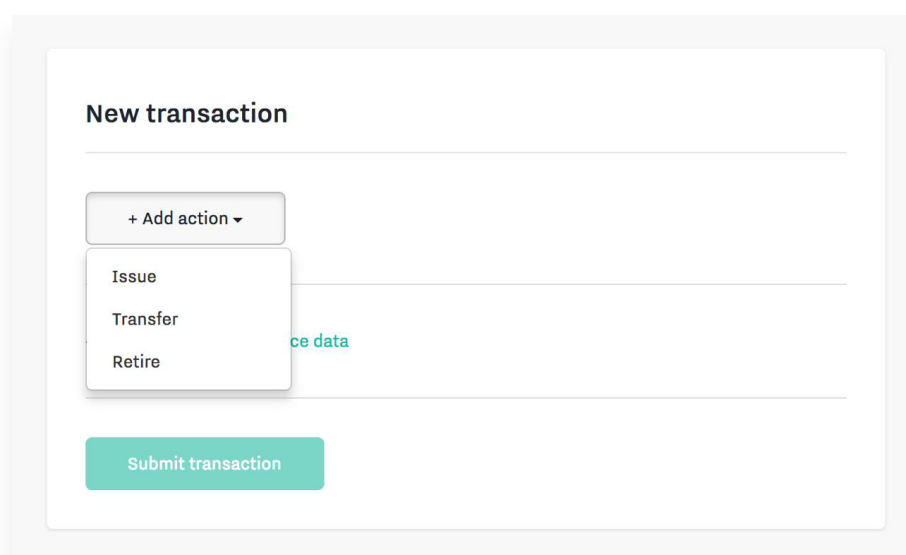
## Developing

As you're developing your application, Explorer is a quick place to execute manual operations for sections of code that you haven't written yet.

For example, you may wish to simulate some new types of transactions as you are working on the UI that displays them. This is easy to do with the transaction builder form.



## Access Control

Access control is defined at the team level. Within a team, you can create people and systems and control their access with roles.

Roles apply to two areas of access:

• **Team dashboard** - available to people via a web browser with an email and password.

• **Ledger API** - available to people and systems via an SDK with an API credential.

## TxVM

TxVM stands for "transaction virtual machine" and seeks to achieve the expressiveness and flexibility of an imperative contract model such as Ethereum's while maintaining the efficiency, safety, and scalability of a declarative transaction model such as Bitcoin's. TxVM defines a stack machine for manipulating basic data items like strings, integers, and tuples, but also specialized types: values, each with an amount and asset type, and contracts, programs that lock up values and other data. Rules governing the handling of these types provide guarantees about integrity and security. Each transaction is a TxVM program evaluated in isolation from the blockchain state and whose output is a deterministic log of proposed state changes for the blockchain. Transactions can therefore be validated in parallel and their logs applied to the blockchain in linear time. Our implementation of TxVM is currently used in production on Sequence, Chain's blockchain-based hosted ledger service.

With TxVM, we seek to combine the respective strengths of the declarative and imperative approaches to representing blockchain transactions while avoiding their weaknesses. It takes advantage of lessons we learned from our previous design, ChainVM, and from developing Ivy, our smart-contract language, which compiles to ChainVM as well as Bitcoin Script. TxVM is designed to be an ideal compilation target for Ivy.

A TxVM transaction is an imperative program that produces a declarative log of proposed blockchain state changes when executed. Execution happens in isolation from the global blockchain state. Running in isolation means TxVM programs cannot have unexpected side effects in other contracts and run in parallel.

Earlier versions of the Chain Protocol (and other blockchain systems) represent transactions with a static data structure, exposing the pieces of information — the inputs and outputs, with their associated fields — needed to test the transaction's validity. An ad hoc set of validation rules applied to that information produces a true/ false result.

In TxVM, this model is inverted. A transaction is a program that runs in a specialized virtual machine that embodies validation rules. The result provides information about inputs and outputs, guaranteed valid by the successful completion of the transaction program.

The "scripts" that in other blockchain systems are used to lock and unlock pieces of blockchain value are, in TxVM, simply subroutines of the overall transaction program. This allows the creation of sophisticated, secure value flows that are difficult or impossible to do otherwise.

## Concepts

The transaction program, together with a version number and runlimit, is called the transaction witness. It contains all data and logic required to produce a unique transaction ID. It also contains any necessary signatures (although these typically appear after "finalization" and don't contribute to the transaction ID).

A witness program runs in the context of a stack-based virtual machine. When the virtual machine executes the program, it creates and manipulates data of various types: plain data, including integers, strings, and tuples as well as special entry types that include values and contracts. A value is a specific amount of a specific asset that can be merged or split, issued or retired, but not otherwise created or destroyed. A contract encapsulates a program (as TxVM bytecode) plus its runtime state and upon creation, must be executed to completion or persisted in the global state for later execution.

Some TxVM instructions (such as storing a contract for later execution) propose alterations to the global blockchain state. These proposals accumulate in the transaction log, a data structure in the virtual machine that is the principal result of executing a transaction. Hashing the transaction log gives the unique transaction ID. A TxVM transaction is valid if and only if it runs to completion without encountering failure conditions and without leaving any data on the virtual machine's stacks. After a TxVM program runs, the proposed state changes in the transaction log are compared with the global state to determine the transaction's applicability to the blockchain.

Learn more about TxVM in our technical paper here: **https://chain.com/txvm.pdf**

## Sequence NFTs

Chain's Sequence NFT product is a managed service that enables any organization globally to launch their own branded and customized NFT solution. Our team provides an end-to-end solution for the design, development, compliance, sale, and utilization of NFTs powered by Sequence. This provides access allowing the management of all transactional data and customization of the smart contract when deployed on a client selected public network bridge.

# Chain Token

**The Chain Ecosystem Cryptocurrency**

## XCN
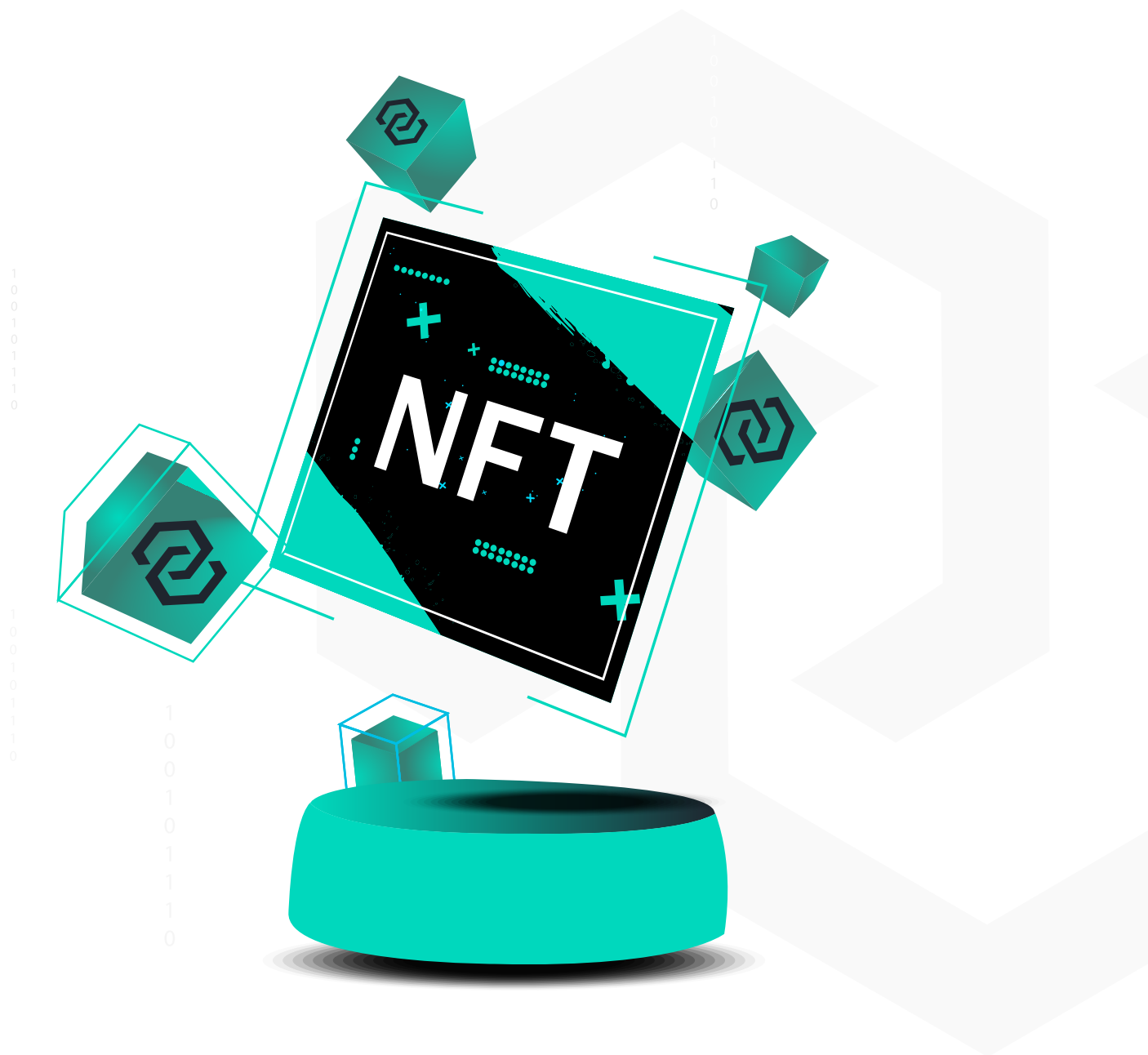
Chain Token (XCN) is the governance and utility token for the Chain Protocol designed to vote on protocol improvements and various community-driven programs through the Chain DAO. XCN is also utilized for node deployment, discounts, premium access, and a payment method for fees on Chain Cloud and Sequence.

## Utility

| Staking | Governance | Payments | Discounts | Access |
|---------|------------|----------|-----------|--------|

## Token Economics

Chain Token has a fixed max supply **53,470,523,779 XCN** units and there is no minting functionality to ever inflate or increase this supply. The token distribution is as followed:

### Circulating

**Amount:** 23,470,523,779 XCN
**Details:** The total unlocked and freely circulating XCN available in the market
**Months:** N/A

0xA2cd3D43c775978A96BdBf12d733D5A1ED94fb18 →

### Company

**Amount:** 15,000,000,000 XCN
**Details:** The Company allocation is set aside for Chain's parent entity and designed to be utilized for corporate operations. These tokens are locked in a Time Lock Smart Contract with a monthly release of 100,000,000 XCN beginning April 2023
**Months:** 150

0x8f6ffec54c1e569c63992eb2dc4fae84e3792551 →

### Team

**Amount:** 5,000,000,000 XCN
**Details:** The Team allocation is the amount of XCN granted to the founders, team members, community managers, and developers of the project. These tokens are locked in a Time Lock Smart Contract with a monthly release of 100,000,000 XCN beginning April 2023
**Months:** 50

0x51f3e348955383f8ad5e1f37f056e8c73dabdf6c →

### DAO

**Amount:** 10,000,000,000 XCN
**Details:** The DAO Treasury allocation is under the control of Chain Governance Stakers who control these funds through community driven initiatives. The monthly budget passed on the last community constitution is 100,000,000 XCN
**Months:** 100

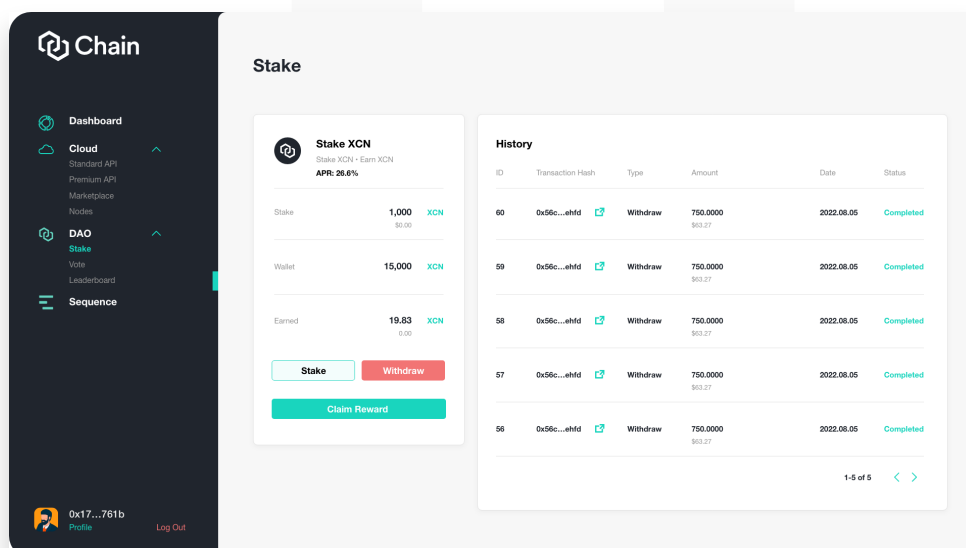0x4d82f8329f308ae8cac6ee38b839611843f5e021 →

## Chain DAO

The Chain Decentralized Autonomous Organization ("DAO") controls the entire Chain Protocol. XCN token holders control the permissionless network through on-chain proposals and governance. XCN token holders also maintain the Chain DAO Treasury.

These parameters are controlled by trustless smart contracts that are audited and secured. For every 1 XCN token, you are given 1 vote. To participate in putting forward proposals and voting for them, users will need to stake their XCN as security in the protocol. Those users earn rewards from the protocol, which the DAO determines through on-chain proposals. The Chain Constitution for the DAO was enacted to set a standard of rules and practices to promote a safe and healthy DAO.

## Staking

In order to participate in the Chain DAO and Chain Governance, users must stake their XCN into the protocol. The Chain Staking contract is a self-custody Ethereum smart contract that gives 1 vote weight per 1 XCN staked. Users who are staking their XCN to secure the protocol receive staking rewards that are set by Chain DAO through governance proposals.

# Governance

Chain Governance is an essential part of Chain DAO where XCN stakers control the protocol through on-chain voting and proposals. The governance smart contracts control the timelock contracts and DAO treasury as well as other protocol parameters such as fees, rewards, and more. Current parameters for launching proposals require 100,000,000 XCN to put forward and 200,000,000 XCN to reach quorum. These current parameters also mandate a 2-day voting period and 2-day wait period before execution on-chain. Proposals that do not require on-chain modification are still needed to go through snapshot polling based on the rules and regulations in Chain Constitution.
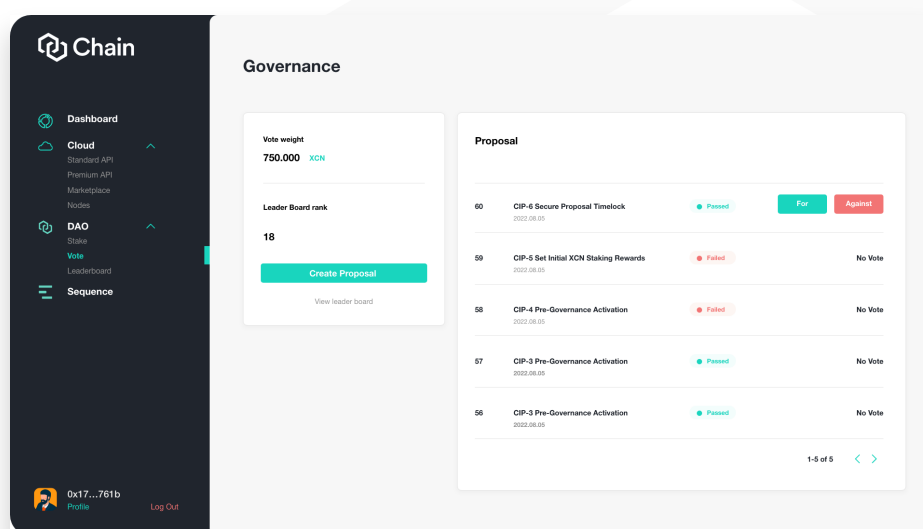
# Chain Gives

Chain believes in supporting individuals and charitable organizations worldwide through the power of crypto and blockchain.


**Supporting Ukraine**


**Working with REFORM**


**COVID Support**

### Impactful

We are on a mission to help countless people worldwide through donations to charitable organizations.

### Difference Makers

We believe we can positively impact individuals and families worldwide through our contributions and the organizations we support.

### Global Reach

With the power of crypto and blockchain, we can rapidly send funds to those individuals and organizations.

# Chain

Join our growing community

Chain.com                  @Chain

blog.chain.com             @ChainOfficial

@Chain                     @Chain

@Chain                     @Chain-global