Chain

An Introduction to Chain Core

The Blockchain Platform
for Financial Services

Chain

Chain Core is infrastructure software that enables institutions to issue and transfer financial assets on permissioned blockchain networks

Built specifically for the financial services industry, Chain Core features:

Financial assets in a digital medium

Designed for currencies, securities, and other issued financial instruments

Instant settlement

Federated consensus designed for immediate transaction confirmation with absolute finality

Permissioned network access

Role-based permissions for operating, accessing, and participating in a network

Scalability and reliability

Throughput to meet market-scale applications and server architecture designed for high availability

An immutable ledger

A perfectly auditable record of transaction activity that cannot be forged or alterered

Transaction privacy

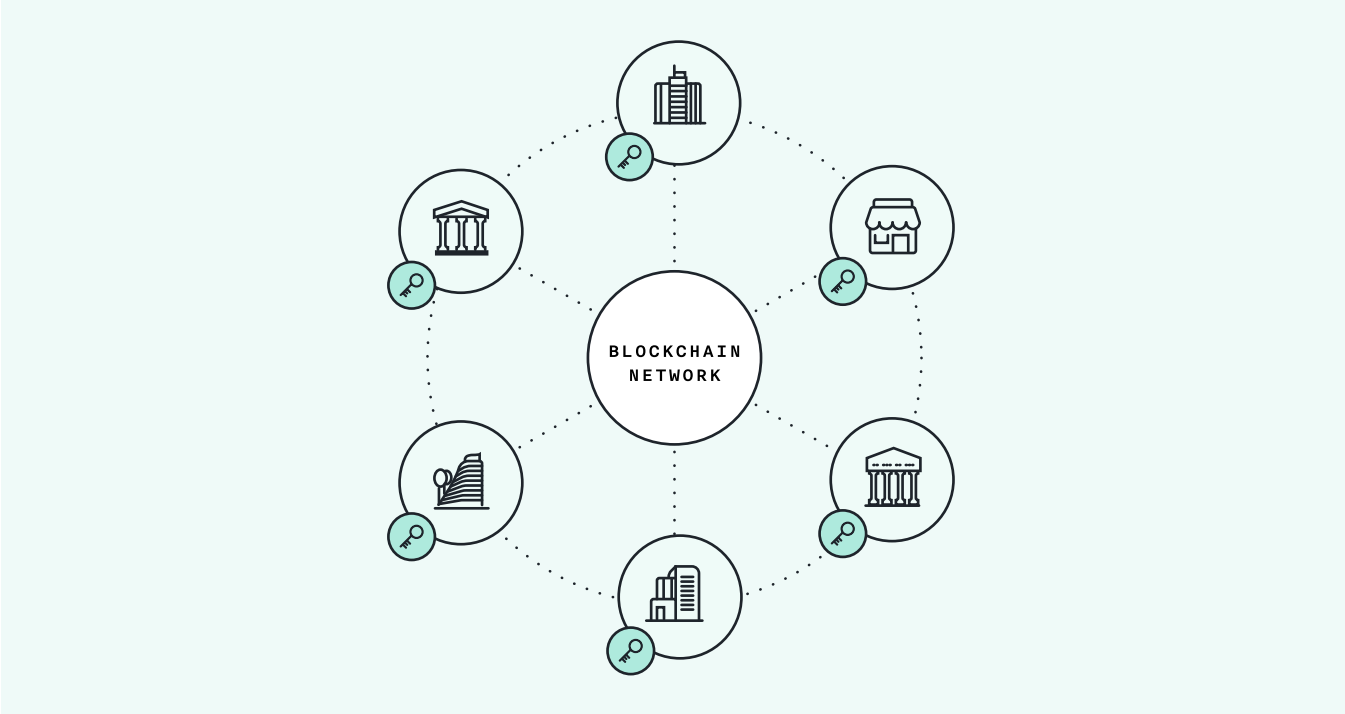
Only the parties involved in a transaction (as well as those they authorize) can view transaction details

Full-stack security

Native integration with hardware security modules, multi-signature support, best-in-class cryptographic primitives, and an auditable, open source stack

Reference data

Assets definitions, compliance data, and arbitrary annotations are included directly in the transaction structure



Cryptographic keys enable participants to move value directly on a blockchain network.

Reimagine the Financial System

Blockchain networks reimagine our financial system in a digital format. Participants on blockchain networks can perform all of the same financial functions that they can today: transacting, custodying, issuing, creating, and servicing assets. But instead of relying on third parties, participants execute these actions themselves, directly to or with their counterparty.

This can be conceived as a novel type of ledger that is shared across entities and enables electronic records to behave like transferable financial instruments, eliminating many of the complex messaging-based systems that are typically involved in clearing, reconciliation, and settlement.

Blockchain networks leverage cryptography to enable actors to control their assets directly and allow participants to validate the entire contents of the ledger. This can be achieved while maintaining the confidentiality of transaction details and the privacy of network players.

Like any financial infrastructure, blockchain networks depend on a purpose-built technology stack. Chain Core is an enterprise-grade solution for participating in or operating a blockchain network.

Rethink Your Business

Chain Core enables organizations to launch and connect to blockchain networks that operate on the open source Chain Protocol.

In order to meet the security, governance, and scalability demands of the financial industry, we developed the Chain Protocol in partnership with institutions including Visa, Citigroup, Nasdaq, State Street, First Data, Fiserv, Fidelity, and many more.

More than a technology, our partners recognize that a blockchain network is a strategy for market transformation and growth.

The following are some examples of the opportunities being enabled by Chain's technology:

- Moving money internationally more quickly
- Transferring securities directly between asset managers
- Building a secure ledger for tracking assets across divisions of a large organization
- Creating a loyalty points system for a group of brands
- Issuing digital gift cards onto a network that can support multiple wallet vendors

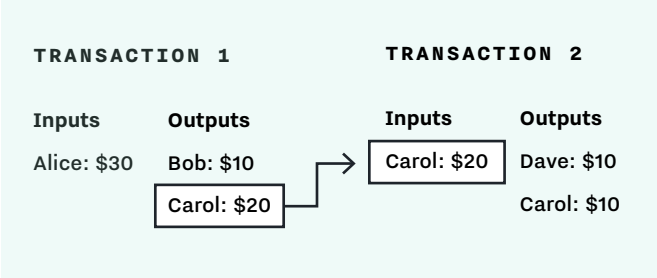
Rethink Transactions

Chain Core-enabled blockchain networks facilitate transactions between entities directly. These transactions can serve to issue new assets, transfer assets between parties, or retire assets.

Each of these cryptographically enforced actions creates a ledger update, or transaction, on the network. The ownership of the assets is immediately updated for all participants. From government-issued currencies to gift cards, Chain Core issues assets into a common, interoperable, digital format.

Every transaction has inputs and outputs. As with traditional double-entry bookkeeping, the inputs and outputs of every transaction must balance. Inputs consist of the initial position of each party involved in the transaction. Outputs are the final position.

Following the issuance of units of an asset, the inputs of every subsequent transaction are derived from previous transaction outputs. These outputs are accessed by the new owner and can be spent.



Cryptographically linked transactions.

Rethink Custody

Chain Core uses cryptographic public/private key pairs to keep track of identities, accounts, and ownership. This system allows network participants to directly control their assets, without relying on a third party.

The public key acts as the address or account number to which assets can be sent. The private key is used by the account owner to access those assets and spend them.

In the Chain Protocol, every transaction executes a programmable script that we call a control program. Control programs consist of the rules or conditions that must be satisfied to access or spend an asset. Control programs are attached to each transaction output and define ownership using these rules. For example, an account control program defines the private key or keys that can spend assets from a transaction output.

Rethink Issuance

Chain Core also allows entities to originate assets and issue them onto a network.

In order to create a digital asset, an issuer first uses a private key to derive a new asset ID. Similar to a CUSIP or an ISIN, an asset ID is a globally unique identifier that represents a set of fungible instruments.

To mint units of an asset, the issuer creates and signs an issuance transaction using the relevant private key, which originates the new instruments into a designated account.

As with asset transfers, issuance transactions are governed by rules in control programs. These could include: requiring multiple signatures for issuance, placing limits on total circulation, or constraining transfers to meet specific conditions. Assets can also include an unlimited amount of reference data such as data hashes, raw bytes, JSON objects, and so on.

Rethink Assets

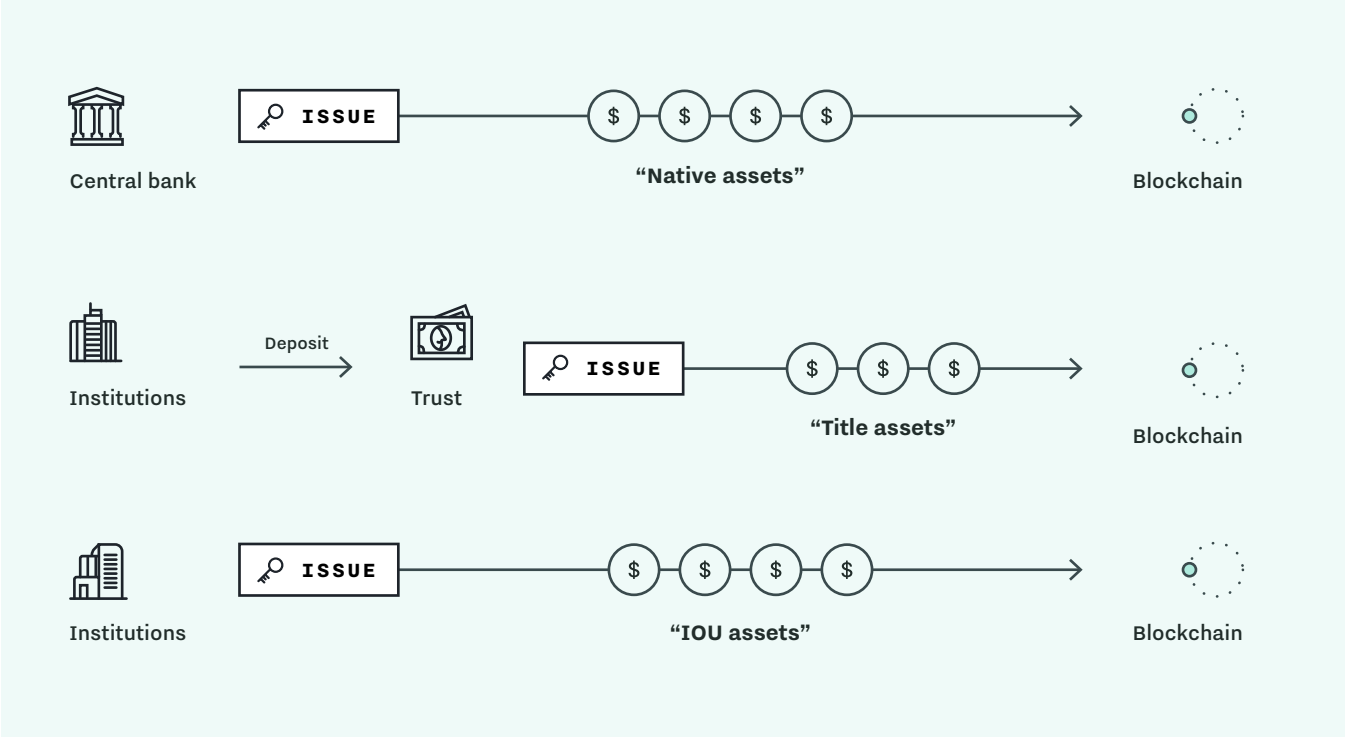
Assets issued on Chain-enabled blockchain networks are cryptographic bearer instruments that act as claims on the issuer. From a business logic perspective, assets can fall into one of three categories:

- **Native assets:** issued directly by the legal issuer onto the network
- **Title assets:** claims on deposits held in a trust by a party other than the legal issuer
- **IOUs:** issued by institutions and represent a liability for the issuer

Whether dealing with currencies, corporate bonds, or gift cards, digitizing assets on blockchain networks opens new possibilities for innovation in financial products and services.

Rethink Financial Services

When assets become digital, financial services becomes software. What role should you play in the emerging digital asset ecosystem?



Where assets get their value.

The Chain Protocol defines three functional roles an entity can play on a blockchain network:

- **Asset Issuers:** define and issue digital assets
- **Account Managers:** custody and transfer assets
- **Observers:** receive blocks and view blockchain data, but do not create transactions

Corporations, brands, merchants, and governments can reimagine themselves as asset issuers. Custodians and banks can transform into account managers on a blockchain network. Meanwhile, regulators and risk managers can reinvent their role with real-time insight and perfectly auditable records.

Any entity running a Chain Core can participate in one or multiple of these roles.

Launch a Blockchain Network

The firm, or firms, that launch a blockchain network in a market are typically designated as the operators of that network. Exchanges, brokers, payments networks, or government agencies are examples of entities that are positioned to naturally adopt the responsibilities of network operators.

Network operators perform four functions on a network:

- Determine who can participate in the network
- Gather signed transactions from participants
- Generate and sign blocks of these valid transactions
- Distribute blocks to participants

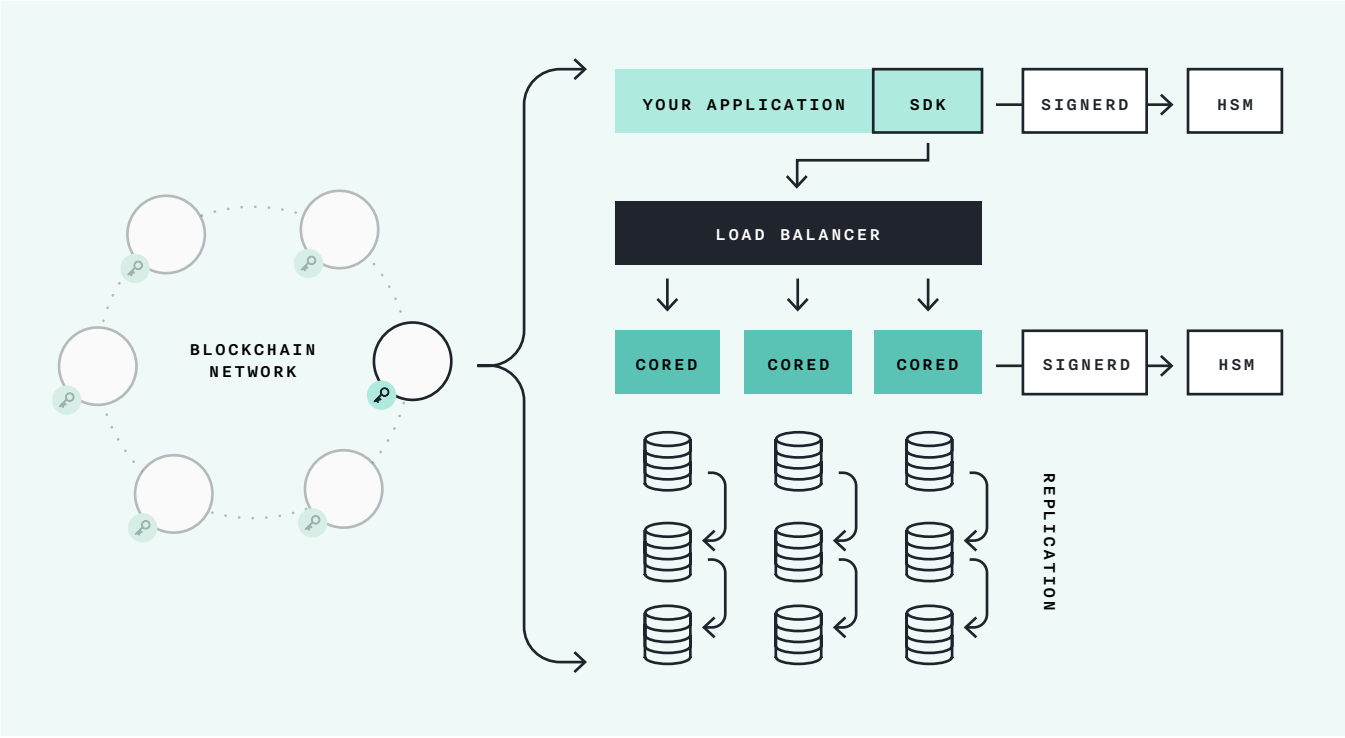
A block is only valid when it is signed by a quorum of block signers in a process we call federated consensus.

All members of the network know the identities of the block signers and accept blocks only if they have been approved by a threshold number of signers. Each network participant can also cryptographically validate the whole chain of transactions. This consensus process ensures that competing transactions are resolved and guarantees that transactions are final.

Operate a Blockchain Network

In order to operate or participate in a blockchain network, an entity runs a node in the network. Chain Core implements the open source Chain Protocol and is designed to run in enterprise IT environments.

Chain Core consists of a storage layer that houses both global blockchain data and local account data.



Chain Core architecture.

On top of this is a services layer that allows for the creation of assets and transactions. Finally, there is a communication layer consisting of an API that connects to applications and links nodes together. Our software development kits (SDKs) allow developers to create applications with ease on top of this stack.

Networks depend on proper management and rotation of key material to secure digital assets. Chain Core integrates with industry-standard hardware security module (HSM) technology. All block and transaction signing takes place within hardened HSM firmware. Multi-signature accounts using independent HSMs further increase security.

Deploy Modern Financial Infrastructure

Chain Core is engineered for the performance demanded by modern financial systems. The time to create, finalize, and settle a transaction is measured in milliseconds. All new features undergo performance testing and optimization to ensure that each release of Chain Core maintains resource utilization and high throughput.

Chain Core can scale to hundreds of servers across many data centers so that the failure of any one component does not impact the health of the overall system. The communication and service layers are stateless and consequently achieve high availability by the simple addition of active redundant servers. The storage layer achieves high availability with a combination of synchronous and asynchronous replication together with a simple failover scheme.

Because its goal is to modernize the backbone of financial services, Chain Core supports today's volume of transactions and beyond. Scalability is a key design principle of Chain Core. Bottlenecks and other restrictions are engineered away to achieve near-linear scaling by the simple addition of hardware. Requests are load-balanced across the communication and service layers. Data is replicated and sharded across the storage layer.

Partner with Chain

In addition to delivering industry-leading blockchain infrastructure software, Chain offers solution design studies, application development, technical support, and network services to our partners that are building and operating production networks.

Chain Core Developer Edition is our free platform for prototypes that is available for download at developer.chain.com.

Chain Core Enterprise Edition is our production software stack that enables our partners to launch, operate, or participate in a blockchain network.

Organizations using Chain Core Developer Edition can purchase monthly support and training retainers to augment their team's efforts and ensure they take full advantage of the capabilities and security features of our blockchain architecture. Enterprise users can access 24/7 operational support with service level agreements.

About Chain

Chain Inc. is a technology company that partners with leading organizations to build, deploy, and operate blockchain networks that enable breakthrough financial products and services. We are the authors of the Chain Protocol, which powers the award-winning Chain Core blockchain platform.

Chain was founded in 2014 and has raised over $40 million in funding from Khosla Ventures, RRE Ventures, and strategic partners including Capital One, Citigroup, Fiserv, Nasdaq, Orange, and Visa. Chain is headquartered in San Francisco, CA.

Learn more at www.chain.com.

CONTACT US

hello@chain.com

FOLLOW

twitter.com/chain

github.com/chain

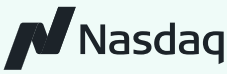
INSTALL CHAIN CORE DEVELOPER EDITION

chain.com/download

READ THE CHAIN PROTOCOL WHITEPAPER

chain.com/protocol

Chain has worked with industry leaders:



Chain