CONDUIT

Conduit Network

Core Services

Core Services Product Roadmap for Mainnet

Author: Conduit Network
May 2024

Table of Contents

Overview

The Conduit Network has two types of physical Nodes, Core Security Nodes and Worker Nodes. Worker Nodes run Smart Meters that measure the use, sale, or transfer of Resources. Core Security Nodes run all of the Core Services of the Network, and must operate at the highest levels of security. These Core Services provide all of the Network's accounting, data management, financial services, identity/security services, and Resource management for all Network Resources.

The Core Services are built on a specialized high security version of Linux that uses the Core Service Authentication and Authorization services to control access to all Resources on the Network. These form an open, Network-wide security infrastructure that was missing from the original design of the internet, and together, they are compatible with current internet protocols.

Everything else on the Network builds upon these Core Services, and anything built atop the Network must integrate and use them to operate. Core Services are designed to enable the creation of a digital society, and establish the foundation needed for Computable Contracting and Statutes, which are key elements of the Network product road map.

At the center of these services is a new type of ledger system that is a DLT of both DLTs and Blockchains. The DLT system is not a single DLT or Blockchain technology, but a merger of almost every DLT and Blockchain technology with the addition of some that are created by the Network itself. This enables the integration of both Web2 and Web3 technologies at the hardware OS level. A Party doesn't need to decide which chain or DLT they want to build upon, they can literally use any or move tokens between them.

This is all made possible by the highly-secured, FIPS/NIST rated hardware, which can be operated in a trustless environment. With the exception of processing-intensive proof-of-work consensus, this hardware can run any blockchain mine, block validator or notary.

Core Services can be thought of as a decentralized OS for a new kind of cloud infrastructure that is decentralized and owned by people. This infrastructure is designed to allow commerce to be controlled at the edge, which only relies upon large, centralized data centers when needed.

These Core Services enable anyone to place a meter on the use, sale or transfer of almost any asset, IP, good or service. These meters integrate with a powerful rewards system to incentivize others to buy, create, or operate new Resources on the Network. This is done in a manner that returns sovereignty, ownership, and control to the people that create the value on the Network – the buyers, sellers, investors and operators that buy, create, use or transfer these Resources, as opposed to accruing the value to a set of passive shareholders. Active creators of the value retain the value created.

Core Services Overview

Core Security Nodes run a decentralized set of services referred to as the L0 DLT. The L0 DLT is best imagined as a new type of trusted internet based on a new type of hardware and operating system that contains an embedded DLT of DLTs/blockchains. This system provides five categories of decentralized services:

1. **Accounting**
    - **Accounting** – Rollup level accounting, order and fulfillment of resources.
    - **Temporal Ledgers** – Party, inventory and accounting entity ledgers.
    - **Secure Storage** – Party's keys and secret information.
    - **Wallet Accounts** – Manage the wallet accounts for all accounting entities.
2. **Data**
    - **Database** – MariaDB database services.
    - **File System** – Manage files and folders for shared access to files (S3 replacement?).
    - **Replication** – Data replication, distribution and consensus.
    - **Messaging** – Publish subscribe messaging queues.
3. **Financial**
    - **Blockchain/DLT** – Interfaces, bridges and tokenization or de-tokenization on demand.
    - **Payments** – All transfers of value, paywalls, exchange and card issuing / processing.
    - **Registries** – Digital asset management.
    - **Treasuries** – Assets custodian via regulatory entities and compliance.
4. **Identity**
    - **Authentication** – Ensure identity for actors is known and appropriately authenticated.
    - **Authority** – Ensure actors only access resources to which they have legal authority.
    - **Profile** – Manage the profile and credentials of all parties (KYC, preferences, etc.).
    - **Resource** – Manage the identity, authentication and verification of all resources.
5. **Resource**
    - **Allocation** – Resource allocation and use, capacity and gaps assessment.
    - **Billing** – The calculation of charges for all Resource use, sale and transfer.
    - **Utilization** - Manage Resource configuration and location to maximize value.
    - **Directory** – Resource name services and routing needed to optimize provisioning.

The following sections cover a more detailed description of each of these core services.

Accounting Services

Network accounting services provide a set of DLT/blockchain based accounting-related services for the Parties, whose respective DLTs are located in a specific Core Security Node. The purpose is to ensure compliance with tax and regulatory requirements, as well as providing automated management of rollup level accounting, inventory, wallet, and other related information for Syndicates and Ecosystems that don't have any dedicated accounting department. These services include the backup and management of secret information and party keys on highly secure devices.

Accounting

The immutable Accounting System is not necessarily meant to replace traditional management accounting, but it does provide GAP or IFRS rollup level accounting using a common Network chart of accounts – and optionally an entity-specific chart of accounts. This system supports a complete general ledger with subledgers. The Accounting System can be used to provide a real-time, automated set of accounts including a P&L, balance sheet and cash flow related to transactions processed on the Network.

Each Party has at least one, but may have more than one, Accounting Entity. Each Accounting Entity represents a separate set of books, which can be built into a tree of books for a single party. Accounting Entities can be used to model departments or subsidiaries, yet they represent nothing more than a subset of the Parties accounting. Accounting Entities can also be used for non-fungible assets to enable fractionalization. Each Party has one root Accounting Entity into which all Subaccounting Entities roll up and consolidate. All Network rights, obligations, or value transfer transactions occur within the scope of an Accounting Entity for all counterparties involved in a transaction.

Ecosystems and Syndicates use Accounting Entities to fully automate all their accounting to enable their operation in a transparent and decentralized manner. Each Ecosystem or Syndicate uses a set of predefined agreements containing the account coding as part of the scripting of the agreement itself. These agreements are like smart contracts in typical blockchains, but are actually defined in metadata vs. code so they are actually smart and can be printed as a physical agreement for use in legal contexts.

Each Accounting Entity supports order management and fulfillment for Resources, complete with inventory, purchase orders, sales orders, and invoicing, which are useful for tax, import, or export invoices. The Accounting System can ingest information from external accounting systems through third-party created Gateway interfaces. Optional modules for the automation of sales or VAT tax are developed by members of the Accounting Ecosystem, and can even make automated tax payments. These tax modules are created and maintained by accounting professionals through Gateways connected to standard software systems via Accounting Ecosystem Syndicates.

Temporal Ledgers

The Accounting Services also provide a set of common ledgers for use by Parties. All ledgers are immutable Temporal Ledgers, which allow a Party to record today any transactions that affect rights or

obligations in the future. This is required to accurately model most real-world transactions like supply chain terms, real estate leases, IP licenses, and financial derivatives or bonds. A Temporal Ledger enables the recording of updates that supersede existing information, or to record transactions that occur on a future date and don't require any additional processing to take effect. For example, a Party can change their address for example and have it go into effect in the future when they actually move.

Temporal Rights Ledgers are one of the most fundamental differences between the Network and traditional blockchains because they solve custody problems. Rights of Possessions can be separated from Rights of Use or Rights of Ownership, which enables their transfer and holding by individual parties for any specified time period.

All Fungible Asset Accounts support temporal, time-based transactions which can be recorded in the future and become effective the moment that time threshold is reached. The Network uses cesium clocks for a dependable, High Trust timesource consensus system that enables Rights to be transferred on a specific date in the future. This effectively enables a locking mechanism without multisig wallets, because the Right of Use itself can be locked without necessarily also locking the Right of Possession or the Right of Ownership.

Temporal Ledgers include ledgers for Accounting Entity, Customer, Supplier, Membership, Agents, Inventory, Devices, Order, Invoice, PayIds, and others. The General Ledger, Inventory, Order and Invoice ledgers all support real-time sub ledgers with atomic subtotals.

Secure Storage

Secure Storage is used to store a Party's keys and all other Party-specific secret information. Parties with their own Core Security Node(s) may choose to store their secrets and keys on their Service Node(s) plus any backup Core Security Node(s) needed to provide recovery. Secrets can be accessed via Web2 or Web3 methods depending on a user set configuration called a Mandate, which controls all access to the private, secret data. No one can access secrets without a Party's permission.

Parties without their own Service Node(s) may choose the jurisdiction and location where they wish their secrets to be stored. The Network will then determine the best Service Node(s) on which to store these secrets. Parties may authorize anyone, but provide a list of Licensed Parties who post a Bond to enable them to recover others' secrets in case they are lost. These licenses are only available to Parties who have passed the High Trust identity verification process and have been Authenticated on the Network consistent with the Parties Agent Mandate.

Wallet Accounts

All Network Wallets and their related transaction information are private. Only a Party that the Account owner allows to act as an Agent, a Treasury, or another Party to whom is granted Authority via a Mandate may see transaction details or the balances. However, the Network can provide cryptographic proofs of these when needed to verify a Party's claims. Wallets store two types of account:

- **Fungible** – Accounts that hold asset classes that are freely exchangeable, such as gold, rice, cash, shares of stock in a specific company, etc., and

- **Non-fungible** – Accounts that hold asset classes where each item is unique and can't be exchanged one for another because the assets are not equivalent, such as real estate, vehicles and NFTs.

Accounts can support any asset class including currency, and can hold mixtures of Assets using the Network's Asset Alchemy process. Accounts can support any blockchain token for which a Network Bridge has been implemented, or real-world asset for which a Gateway exists. Wallets use Registries for digital assets that have no regulatory requirement and Treasuries for real world assets that require regulated entities to act as custodians.

All Fungible Asset Accounts support the separation of the four property Rights (Ownership, Possession, Use and Destruction). This enables the Party controlling each Right to be separate so that the respective Rights may be held by different parties, which effectively solves the custody problem with digital assets. This also enables the modeling of many things in the real world within existing contract law wherein these Rights are commonly separated in the language contained within agreements. For example, this enables the Right of Use to be held by a different Party than the Right of Possession which locks the Assets from being moved until the Right of Possession is transferred, but still allows the asset Ownership to be transferred.

Any asset in an Account may be Tokenized on Demand to another blockchain or within the Network. Wallets that also support the Tokenization on Demand of specific Rights of an Asset on another blockchain, but doesn't necessarily need to Tokenize them to transfer them on the Network. The reverse is also true as any tokenized asset supported by a Trust Bridge can be moved to the Network or another blockchain through the Network via another Trust Bridge.

Wallets are recoverable if lost, and can be configured to require specific devices be used for authentication, or even require various forms of human or multi-factor authentication processes called Mandates. Mandates use a problem domain-specific language for Authority, which allows a wide variety of Account specific Authorization processes to be defined for execution of transfers or purchases based on amounts or sum within a period.

An Accounting Entity's Mandates and its Secret Store are managed by Wallets. Mandates can be used to enable the recovery of lost Secret Store Keys as well as Wallets. Wallets act as a hardware Wallet that can be fully backed up and recovered using a Party's own or standard Mandates to control how a Party must be Authenticated in order to take specific actions.

Data Services

The Data Service manages the cache, consensus, indexing, and replication of objects, ledgers, records, databases, and files. It also provides a standard messaging architecture and service through the publication of subscription services. These data services run on all Core Security Nodes and Worker Nodes, however they are used for different purposes in each Node category. Data Services operate as an infinite number of different DLTs all linked together via intersecting hashes.

The number of Nodes in a specific DLT depends on both its purpose and the Party's wishes. Very few things need to be infinitely replicated to exist on all Nodes, and furthermore, trust is not increased by adding more Nodes vs. hashing together many independent things in interconnected graphs. The

existence of High Trust hardware makes the possibility of a 51% hack impossible both economically and physically, which opens up new approaches to how consensus can be achieved.

Data Services make full use of the new decentralized reality that High Trust hardware enables. As a result, the Network can support transaction volumes and speeds, which would not be possible in normal blockchain or DLT environments. Every Party has their own DLT, which is hashed together with every counterparty's DLT on at least 4 other Nodes for a total of 5.

Therefore, every piece of data that is on the Core Secruity Node for a Party is also on their:

- Treasuries or Registry Core Security Node,
- A Counterparty's Core Security Node for all of the transactions with that counterparty,
- A Counterparty's Treasuries or Registry Core Security Node, and
- at least 1 other Core Security Node.

Parties can set the requirement for up to 1,000 Core Security Nodes and any number of geographic locations by country in order to achieve consensus for their transactions. However, this increases the transaction cost and latency of a transaction. Anything over 11 Nodes in 5 countries is unlikely to be needed because nobody actually ever knows which Core Security Nodes hold what data.

Database

The Network provides a set of database services used by all Core Services. The Network uses a Hashed Event Store, which is conceptually a merger of a Merkle graph and an event store to ultimately create a Hashed Event Store. This Event Store is designed for high performance and it immutably stores temporal objects. The Network uses an extensible architecture for database drivers, but natively uses MariaDB database services at this time.

Services using the Event Store must be written in the Core Services language ESSL. All ESSL generated Core Services are accessed using GraphQL. All Event Stores store the ESSL objects, which all have a unique GUID that acts as its internal Object ID. These IDs are not designed to be used externally because they are more like IP addresses and used between services.

There are three types of Database Services:

- **Network** – based services logically exist on every Core Security Node, but in practice are cached to the Core Security Nodes actually using the information. They also reside on a smaller set of Master Nodes. Therefore, the database does not exist on any single Core Security Node; only parts of the database exist on any Core Security Nodes with specific Core Security Nodes acting as the Master Node for the data object. A Master Node for the object must be used for all object updates, but a cached version can be used for all read operations. The Master Nodes for an object are automatically determined by querying a Master Node ID for the object.
- **Party** – based services objects migrate over the Network to the Core Security Nodes where they are most commonly used, or they can be permanently homed to a Party's personal Node(s) if desired – however this can reduce that Party's transaction performance in some cases.

- **Resources** – based services are located on the Services Nodes used by the Worker Nodes where the Resource's Smart Meter is located. Depending on the type of Resource, one or more Worker Nodes may run Smart Meters for the Resource. For example, the Use Right to a piece of real estate offered for rent could be managed by multiple Worker Nodes because it does not require physical monitoring of the Resource. But the monitoring of a refrigerated warehouse would require multiple physical sensors in the warehouse that verify the content and the temperature of the warehouse in multiple, internal locations.

File System

The Core Services File System manages a global directory of files, logical folders and their respective Node locations. This system is similar to AWS S3, but can also be used by apps, Smart Meters, and Resources Nodes to manage file names and locations within one or more logical tree structure(s). All files are encrypted at rest with the keys stored in the Secrets Store of the Core Security Nodes supporting the Resources location(s) or the Party to whom the file belongs.

Files may have any number of identities within a namespace. Therefore, a file identity could be a URI in one namespace and a GUID in another, but still reference the same file.

Folders are purely logical constructs, and exist for all Parties as a convenient way of organizing files related to a specific Party's activities. All Parties control all access to their files and can define where their files are stored geographically, how many nodes it is on, and what Trust Level of a Worker Node must be used for the storage. All of these affect the cost of the file storage.

Since the keys to the encryption of a file are controlled by the Core Security Node, all encryption and decryption is authorized through a Core Security Node, which also controls all file access control information. This allows the file system to support both private and public files such as websites.

The File System supports a Party-specific access control list and even the Network itself cannot decrypt a file without a User's permission. Like all other Network Authorization processes, file Access Control is managed via Mandates.

Replication

The Replication Service manages database, object, file, and container replication, distribution and consensus. Should any data of any type require any replication, that is managed by the Replication Service, which supports a variety of replication techniques that can be used by developers of Apps, Predicate Proofs, Smart Meters and Trust Bridges.

The Replication Service also manages the consensus between Nodes that host the Network DLTs. The Replication Service uses multiple types of consensus protocols. High volume consensus for economic activity, is handled differently than consensus for slowly-changing, broad distribution information.

Messaging

The Messaging Service enables Billing, database updates, object change, Predicate Proofs, Smart Meters, transactions, and Trust Bridges, to publish messages to a messaging queue. Services, Apps, and Parties with the proper Authority can subscribe to, and receive these messages. For example, this can be used to keep analytics databases or indices current for use by reporting or analytic services. It can also be used to queue tasks for a Party, or also exceptions that would need an Agent's or User's attention.

The Messaging Service does not use consensus, but uses the RabbitMQ messaging protocol, and depends on the Trust Level of the Node where it publishes or subscribes to provide trust. Therefore, the Messaging Service is fully compatible with Web2 applications and services designed to use the RabbitMQ messaging protocol.

Financial Services

The Core Services layer provides a set of infrastructure to support financial transactions via the Network. These services address a critical deficiency in the original internet, which are protocols for financial transactions.

Blockchain/DLT

Trust Bridges only run on High Trust Worker Nodes. They operate as bridges to and from other blockchains or DLTs. Trust Bridges use a special class of Registry Account Ledgers that run on a Core Security Node. These special Account Ledgers control the Right of Possession to the digital assets that have been migrated to, or from the Network. The digital asset can't be moved off the Network or chain until the Right of Possession is restored to the ledger initiating the transaction.

Only a Party with the Right of Use and Right of Ownership Rights in their Wallet can restore the Right of Possession with a Network transaction. This design makes it economically and physically impractical to hack because two Network Parties on two different Core Security Nodes would have to be compromised simultaneously.

Trust Bridges don't just deal with digital assets, but can also be used to migrate data and secure validators running on Enhanced Trust or High Trust Worker Nodes. This enables validators or notaries of other DLTs and blockchains to mine Network Assets by offering cloud based computing services to run the validators or mines on Worker Nodes. The Trust Bridge ensures the validator or notary is running the proper version of the validator or notary via hashes of the container, and deploys new versions when approved.

Registries run by Blockchain/DLT Services use Trust Bridges to support the Network's ability to tokenize or de-tokenize any Network-based assets on demand to any supported DLT or blockchain. This enables many different types of real-world assets or Resources with Smart Meters running on High Trust Worker Nodes to tokenize on demand. This could be anything from a bond to a warehouse receipt. This process also supports the Separation of Rights so that a custodian, logistics service

provider, or warehouse may retain the Right of Possession while the Right of Ownership or Right of Use is separately tokenized and exchanged.

Payments

Payment Services support all transfers of value via the Network, Trust Bridges, or Gateways – and can be executed via any Accounting Entity via its Wallet. Payments can also be recorded in advance and stopped if the fulfillment terms are not met based on the rights granted in a Mandate. Payments support the concept of an escrow, which locks the assets in an escrow such that only when an event is triggered by a Predicate can the final transfer of value occur. This process requires no intermediary, but can be configured to work with intermediaries where human judgment is required.

Payments also support a universal payment addressing scheme called a PayId. A single Party can have any number of PayIds at any time. PayIds support multiple schemes – each allowing for a unique payment identifier to be created by a party that routes the payment to an Accounting Entity and a Wallet Account. This Wallet Account can be native to the Network, or can be an account that is accessed via a Trust Bridge on another blockchain, or through a Gateway to a financial services provider such as a bank.

PayIds can be redirected to another Accounting Entity or account at any time without anyone else knowing if it is for the same Party. PayIds can be used to make payments anonymously where desired because PayId schemes exist that do not have any implied meaning. In addition, there are PayId schemes that allow the use of an email address or phone number, but the Party must prove these are under their control on a periodic basis. Once a PayId is used by one Party, it can't be used by another party until it expires.

The Network also supports its own virtual or physical card issuing system for a native Network equivalent of a rewards card that can be used as a PayId or to make payments via Network Rewards. This system works on any Network-enabled App or website, and can be integrated into any Network-enabled service or Resource for payment. Reward Cards and Wallets can even be used at merchants to receive payments using a PIN, or can be integrated with their own rewards system while avoiding credit/debt card merchant fees.

Using Gateways, credit/debit card issuers can issue credit/debit cards that work on the Network, but have no interchange fee for the merchant when used in Network while also still working on other credit card issuer's rails as well. The funds saved on interchange fees can be used to buy CROP, which mines CNDT and Squares that can even be shared with the merchant or customer. Finally, these cards can also be used without any intermediary for gift cards from merchants with all of the proceeds going to the merchant who carries the liability.

Registries

Digital assets can be used to release net new value if the asset is able to support Rights and Obligation management. This is handled within the Network via Registries. The easiest way to understand this is the difference between the Right of Possession held by a custodian and the Right of Ownership itself, which is held by the owner. Until these Rights are merged, the digital asset cannot be transferred or

traded, but even so, the party with Possession doesn't need to be a regulated institution because it all achieved via technology alone when there is no physical asset.

Registries store the information about the holders of the digital asset's various rights during a given period of time, now or in the future. Registries record which assets have been placed on which chain, and also what Rights have been transferred through a Trust Bridge. They lockup the underlying assets in wallets or smart contracts on the native chain when assets are moved to the Network. Only the Registry has the keys to these blockchain wallets, and they never leave the secure store.

To further distribute the risk, Registries are globally distributed across the Network, and can even migrate from one Core Security Node to another Core Security Node over time. Only Core Security Node directory services know where Registries are located, and no single Core Security Node holds all of the value in a single wallet.

Registries also hold a record of all Network Digital Asset transfers because they act as one of the counterparties in each transaction that transfers the assets. This means all digital asset transfers go through a Registry, which also can hide the identity of the counterparty when so desired.

Treasuries

The function of a Treasury and a Registry is almost identical except that Treasuries work with regulated assets. Asset custodians requiring regulatory licenses use Treasuries instead of Registries, which provide the additional features needed by regulated entities.

Though Treasuries aren't necessarily banks, they can all operate like a Neo bank with all of the modern services like wallets, ATMs, debit cards, checks, and electronic payments. They are also compatible with traditional banks and payment networks through Network Gateways. Treasury Services enable trusts, custodians, and non-bank entities to work with traditional banks, credit unions, and building societies to offer integrated services via the Network through Gateways. Value stored in a Treasury can be accessed within the Network in the same manner that any value otherwise stored in a bank can be accessed.

Treasuries enable a new form of value store based on an age-old model that does not require lending, and can store value in real-world assets instead of just currency. All Treasuries must support the redemption of the assets they store so the underlying assets themselves can be retrieved. Therefore, Treasuries are ideally suited for creating high-rust flat-coins or real-world asset-backed digital assets.

The Network uses Treasuries as an alternative to traditional banks because aTreasury can store value held in, or represented by the things that both businesses need to operate and people need to live. These are things like food commodities, metals, energy, select liquid securities and select currencies. Treasuries must post a bond in the form of Network assets and they earn revenue via transaction fees, the operation of Gateways, conducting arbitrage, creating options, and the mining of CNDT. Core Treasury services enable new business models for financial institutions and regulated custodians by enabling new sources of revenue through connecting real-world assets to the digital world.

Identity Services

Identity Services provide a common set of methods for authentication, authorization, Party profile management, and Resource identification. These IDs use the Identity Service's Directory Service to resolve identity schemes into GUIDs, also similar to how DNS is used to resolve URLs to IP addresses. They also form the security infrastructure for a new version of the internet with native security from the hardware on up.

Authentication

The Authentication Service supports both Web2 and Web3 concepts of identity authentication, but moves them into an Oauth2 token beneath the surface. All authentication must be conducted via the Network supported authentication methods. It uses open and extensible services that must first be audited before being authorized to execute on Core Security Nodes. This service uses OpenID Connect (OIDC) protocol to allow app and service creators to utilize the Network-provided Authentication Services in Web2 environments.

The Authentication Service not only authenticates user login identity, but also authenticates devices such as Nodes on the Network, as well as the devices used by users to login to the Network. Each Party can have any number of Login Identities, each with various levels of trust. This enables Parties to work with simple Login Methods for every day tasks that don't require significant security, and then upgrade their login to more secure, but more time-consuming or device-limited methods in order to enable other tasks.

Each Party can enable multiple Actors, which can be forms of themselves, other Parties, or automated systems such as an AI agent or assistant. Each Actor can have any number of Login Methods, each which enable a different set of actions.

Authorization

The Network is designed to enforce decentralized authorization based on Legal Authority Rights. A Party's Legal Authority establishes their authority, which differs from access control lists (ACLs) or role-based security. This is similar to the systems used by the U.S. strategic nuclear command, which must operate a decentralized authority enforcement system to control its nuclear arsenal.

Anything a Party is permitted to do is based on their Authority Rights granted by Parties in the Network under the Network governance, which descends from a Network Constitution. Mandates are used to grant legal authority to do things, control the scope of the authority, and define the Resources the authority is granted over. These Mandates then convert the legal authority into the roles or access control lists that ensure the security systems honor the legal authority.

This is a two-way, round trip projection that enables the automatic audit of the security via the legal authority. All access is controlled through Core Security Nodes, and is automatically re-validated when Oauth2 tokens expire, which enables a change in legal authority to be enforced as soon as the token

timeout occurs. Even queries are directed through Core Security Nodes so that access to various attributes of objects can be controlled via authority right access configurations.

All Core Security Nodes and Worker Nodes respect Legal Authority Rights, so even the right to update Core Security Nodes with new versions of code must have the valid legal authority under the Network Constitution governance to conduct the activity.

Profile

The Profile Services enable Parties to make and maintain claims about themselves, as well as provide one or more claim proofs, which can then be validated by one or more other Parties. This includes credentials of all Parties for KYC/KYB, which may be done via multiple Parties – each with their own policy. As more proofs are collected and validated by more Parties, the strength of a Party's Profile increases.

The Network enables decentralized Licensed Roles known as Administrators, which carry significantly more weight on verifications than normal Parties. These Parties must go through periodic training and post a Bond using Network Assets to play these Roles. Parties can provide cryptographic proofs based on their profile information without leaking the underlying information, or they can issue Mandates with time boxes around the ability to access the information.

A Party's Profile also supports their preferences, shipping addresses, notifications, and task queues. The Profile is utilized to establish Accounting Entities, manage PayIds, customize the chart of accounts, and other configuration management tasks.

Resource

The Identity Resource Service manages the identity, authentication, and verification of all Resources, App or Services, Smart Meters, Trust Bridges, Gateways, as well as the Worker Nodes themselves. This includes the Profile identity of Devices that Users use to access the Network, which aren't technically Resources in the Network, but rather are those used to access the Network or verify identity.

This service also manages the release and updating of App or Services, Smart Meters, Trust Bridges, Gateways, and the Worker Nodes, with the addition of any verification that these are running the correct version before allowing utilization.

The Identity Resource Service has contextual awareness of which Worker Nodes and Smart Meters monitor which Resources. This includes the Resource Profile, which has the necessary information about the Accounting Entity that owns the Resource, and which Predicates are associated with the Smart Meter monitoring the Resource. The Resource Profile is used by the owner of the resource to configure and control pricing for billing.

Resource Services

Allocation

Being one of the most important services on the Network, the Allocation Service manages the allocation of, and access to, Resources such as Worker Nodes. This service also manages the capacity and gap assessment for Resources on the Network – both geographically, by Trust Level and Service Level.

Therefore, the goal of this service is:

- The allocation of Worker Nodes and other Resources to sufficiently meet the demands of users as near the point of use as possible by taking into account the Resource's current capacity, along with the Service Level and Trust Level required by the user or customer.
- Identification of overly-scarce Resources on the Network, which would benefit from Network Fee increases to encourage Operators to make additional investments, or to identify opportunities to reduce Network Fees to normal levels as a sufficient supply comes online.
- To manage available capacity on the Network by activating Performance Incentives, and also publishing metrics to the market to provide feedback on Service Level, locations, Node Type, Trust Level, and Resource Class that are in peak or growing demand.

In order to accomplish these goals, the Allocation Service can trigger the Utilization Service to move the things that execute to better locations in order to achieve the best overall performance result – giving priority to the highest economic value for the Network's Participants.

Billing

The Billing Service handles the calculation of all Pricing and Billing for the Network. This includes the use, sale, or transfer activity Pricing and Billing for all Network Resources and Network Fees. The service uses a pricing and billing language that refers to the values in Network Events defined by Predicates to calculate the Price and manage the Billing.

Billing can be:

- **Real-time** – the transaction will not complete unless the Billing process is successful,
- **Near-time** – the transaction proceeds, the Billing process is assumed to be successful, but the session token will be invalidated by the Core Security Node if the process fails.
- **Periodically** – the transaction proceeds, and only if the billing period expires and fails to succeed will the session token not be renewed by the Core Security Node. real time, batch, periodic or threshold of cumulative value based. Periodic Billing supports both:
    - Period based Billing – such as once a week, or
    - Threshold based Billing – such as when the amount due exceeds $10.

When a tax Gateway exists, the Billing process can also support the creation of a tax invoice based on the location of the buyer and the seller which incorporates the tax rules between the jurisdictions involved.

Invoices are automatically sent to the Accounting Entity of the Party to be Billed, and can be settled via:

- **Auto pay** – the invoice being received automatically withdraws from the Party's PayId account. Auto pay can only be configured with the prior consent of any Party' being Billed. All payments are conducted in CNDT. When payment must be made from a different store of value, the Network automatically converts the store of value into CNDT for payment via a Gateway. If the payment is not real-time, and there are sufficient funds in the Wallet Account connected to the PayId, a hold is placed on assets in other accounts until the bill is satisfied and a current payable is recorded in the Account Entity General Ledger.
- **Manually** – the invoice is sent to the Accounting Entity for the Party's PayId, recorded in the payables ledger, with a liability being recorded in the General Ledger. The Party must take action to cause the payment to actually be made. If payment is not made within the grace period of the due date, the Party loses the ability to make further transactions until the payment is made.

Utilization

The Utilization Service manages where things execute in order to achieve the best overall performance result – giving priority to the highest economic value for the Network's Participants. As a result, lower Trust Levels requirements may run on higher Trust Nodes if excess capacity exists but never the reverse.

The Utilization Service also distributes Resources to Worker Nodes and Settlement activity to Core Security Nodes so that Resources and Worker Nodes receive a balanced share of activity that produces mining. This includes management of Resource configuration, Node Type, Service Level, Trust Level, and location to maximize value.

Directory

The Directory Service provides a new name resolution and routing service with greater precision and fidelity than traditional DNS. It resolves names like Resource names or Party Names to the corresponding Nodes that host the services, and provides the routing needed to optimize provisioning and load balancing. This means that no one besides the Network itself and the Operator know the location of Resources or Nodes.

Due to GDPR or similar regulatory requirements, the geographic location of all Core Security Nodes must be known. Due to tax and legal requirements, the physical location of Worker Nodes must also be known. Therefore, the Directory Service tracks the physical locations of Nodes, but this information is not publicly available.

The Directory Service supports name schemes that can resolve to various identities. These can be as foundational as the GUID for an object, file, Party, or Resource or Node. Objects or files within a Party

will resolve to the identity of the Nodes with copies of the Party's data for lookup and query execution resolution, or their master Nodes for addition, depreciation, or update.

Directory Services mitigate the ability to conduct DDoS attacks because it acts as a reverse proxy service to the Network. It provides Network-wide content delivery services, and acts as the single point of contact for websites and URI resolution. Finally, the Directory Service provides Network wide VPN services to enable secure point-to-point Network communications.