CONDUIT

Conduit Network

Mainnet

Workers, Smart Meters, Nodes & Core Services

The services and design specifications for Conduit Secure and Worker Nodes

Author: Conduit Network
May 2024

Table of Contents

Overview

The Conduit Network mainnet depends on the use, sale or transfer of Resources that generate revenue. This revenue drives purchasing of CROP, which mines CNDT. The use, sale or transfer of these Resources causes CROP to be contributed as part of the Billing process for these Resources. Any economic transaction related to a Resource can produce a mining event for CNDT or Squares as long as it results in the purchase of some amount of CROP. All Parties have an equal likelihood of achieving a mining event because this is based on the next threshold of CROP purchase being achieved by each party - as opposed to just providing processing power.

The measurement of the economic activity is done via a mesh network of decentralized Nodes running one or more Smart Meters. Smart Meters are oracles, either automated or human, that record events and measurements. Along with their corresponding measurements, these events are recorded in Event Ledgers. Event Ledgers provide the variables needed by Predicates to determine if a State Change has occurred. Predicates are used to provide cryptographic proof that an event has occurred.

Event Proofs can trigger actions that result in:

- The Billings of one or more counterparties for a Resources use, sale or transfer.
- An exception or error being routed for human inspection or automated intervention.
- The triggering of another action.
- The notification of one or more Parties or Agents

The key to Network growth is accumulating as many Resources as possible. Then, enabling the Parties that wish to use, buy or transfer these Resources to do so through the Network.

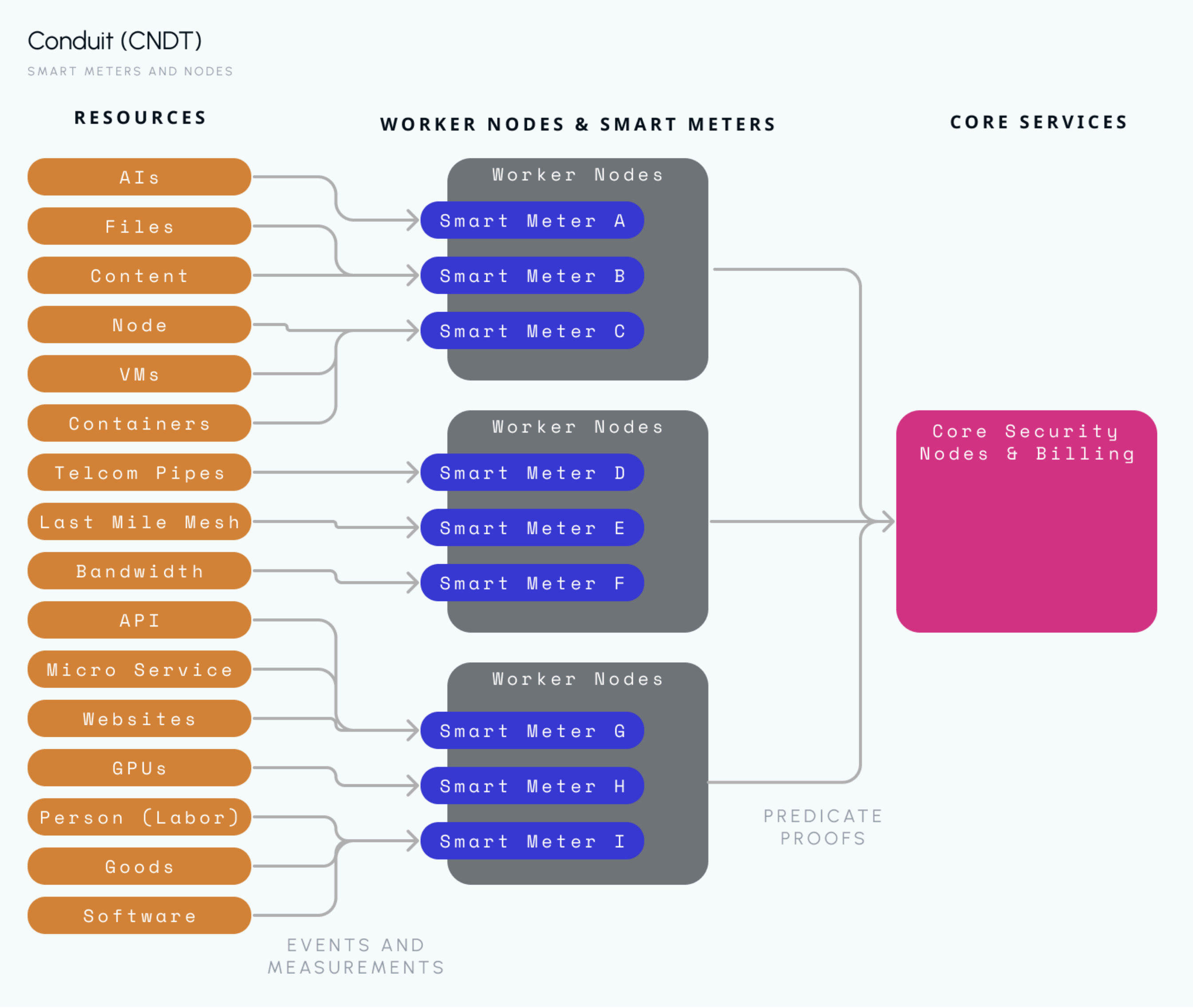
Therefore, the Network is nothing more than a pool of decentralized Resources available, and the Parties willing to pay for their use, purchase or transfer so that CROP is purchased as a result of the respective transaction. This results in all Parties involved in a given transaction participating in the mining of CNDT.

Resources are monitored by Smart Meters, which are a special form of Smart Contract that acts as an oracle to the Network. These Smart Meter oracles use configurable Predicates to recognize a meaningful State Change in Network monitored Resources. This results in an Event Proof being placed in a Core Security Node message queue, which uses a Network Petri Net. This Event Proof is then made available to any subscriber authorized by the Resource owner.

Smart Meters and their Predicates run on Nodes, which monitor the use, sale or transfer of Resources. Therefore, Nodes are devices with the hardware and software needed to automate the recording of events or measurements. Smart Meters running on Nodes notify a special class of High Trust Nodes called Core Security Nodes whenever a Predicate indicates a significant event has occurred. These Core Security Nodes use hardware rated for the most demanding, trustless environments.

Anyone participating in the creation of economic activity resulting in CROP participates in the mining of CNDT. This includes the Resource providers, Node Operators, and the Network's customers

(Participants). In addition, Core Security Node operators earn fees that operate similar to traditional blockchain network gas fees.



Levels and Categories of Nodes

There are four levels of trust for Nodes:

- Low Trust,
- Standard Trust,
- Enhanced Trust, and
- High Trust Nodes.

In addition, there are two categories of Nodes:

- Core Security Nodes, and
- Worker Nodes.

Only High Trust Node hardware can be used to operate a Core Security Node. Worker Nodes operate within any of the four Trust Levels. Resource Owners and their Network Users determine which level of Node is required for a given transaction. In other words, the Nodes that run the Smart Meters act as oracles for the Resource.

Therefore, the highest minimum requirement for either the Resource Owner or User determines the minimum level of Node Trust required for a Resource's use. For example, a Resource Owner may require at least a Standard Trust Node to run Smart Meters that monitor the Resource but a User may require a High Trust Node. In this case, only Resources on, and Metered by, a High Trust Node would be used for that User's transactions.

This enables Resource Owners and Users to choose the level of Network trust and security they desire. Higher trust and security frequently affects cost and transactional friction. Higher levels of trust secure the software, data and hardware from unauthorized use, error, access or fraud. This provides a Network of Nodes and Resources that can be used in transactions with variable degrees of trust based on the desires of the consumer and the owner of the Resource, along with their respective tolerances for risk, as well as the cost / friction associated with corresponding levels of trust.

Finally, the Network is designed to provide any Party with the benefits of cloud computing but still maintain sovereignty over their own data, processes, and assets. This means no one, not even the Network itself, can access data or processes without the Resource Owner or User's permission.

Network

The Network is designed to be an ecosystem of sub networks and resource clusters that forms a new type of highly-decentralized, cloud-based internet owned by its users and creators. It represents a new internet that has governance, security, finance and commerce built into the core of its architecture, wherein the current internet does not. The Network, being wholly comprised of Clusters of edge Nodes, has no centralized entities.

These Node Clusters can consist of small, consumer-level edge Nodes in homes, all the way up to major enterprise data center Nodes with intermediary configurations to meet the specific needs and use cases. Irrespective of size and processing power, Nodes operate in Clusters that Node Operators choose, not the Network. This means a Cluster could be a group of family members or friends, a set of businesses, a club, a business network, supply chain, or simply a DAO or Syndicate.

These Nodes can be computers, communications links or other devices running Smart Meters that monitor Resources. All Nodes are compatible with the existing internet, but can also use new, more secure computer networking technologies between themselves, or when hosting Apps or Services used by Network Users. Nodes can even run existing Layer 1 blockchain validators or mines.

However, the Network is not an internet replacement, but a purpose built iteration designed as a digital economy that rewards everyone that creates, operates, records Resources on, and uses it. Unlike the current internet, which is increasingly controlled by centralized parties, the Network is economically engineered so that it is unfeasible for it to be controlled or operated by large, centralized Parties as it scales.

This is accomplished through Two methods;

- **Economic Incentives** – Edge Nodes are run in small businesses and homes and uses existing electrical and communications pipes plus deploys new pipes. These locations pay nothing extra for real estate or communications therefore it is cheaper and runs on lower cost hardware for the same level of compute as a rack mounted server in a data center. Therefore, the closer to the edge and the smaller the unit the more economical it becomes and the better the service performance due to lower latency. This means that edge devices can offer lower cost and higher performance for many applications which favors the smaller parties. Running a tier 4 data center is extremely expensive but running a tier 4 edge Cluster is much lower cost.
- **Mining Incentives** – The Network uses a pool of 10% of all mined CNDT to offer Performance Incentives to Node Operators that place specific Nodes types in geographic locations where they are needed. One of these locations is within neighborhoods, business districts, or rural areas where no data center would make sense. These Nodes run mesh WiFi, small cells and edge computing in locations that no centralized entity can operate because it is on land that is held or controlled by individual parties. This means it is more profitable to run edge Nodes because they are subsidized.

The backbone of this new internet is made of special Nodes called Core Security Nodes. These decentralized Core Security Nodes have three primary use cases:

- **Sovereignty** – Owning a Core Security Node for your home, office or a trusted circle that is used to create digital and asset sovereignty,
- **Profit** – Operating a shared Core Security Node for others who use it to record their mining transactions in which the Core Security Node's operator has an economic participation, or
- **Convenience** – Owning a mobile Core Security Node device for convenience when conducting transactions from personal devices, such as a smartphone, which acts as a hardware wallet.

Core Security Nodes must be paired with one or more Worker Nodes to mine CNDT. However, Nodes come in form factors that include both categories of Nodes within the same unit or composable stack. Worker Nodes need Core Security Nodes to perform:

- Authenticate and authorize,
- Resolve identifiers and conduct routing though secure communication circuits,
- Accounting, billing and the payments needed to mine.
- High security storage of keys and secrets.

Network Design

The decentralized Network comprises Nodes that are interconnected through a mesh of communications channels and common orchestration frameworks, operating system, and an OS-based DLT of DLTs running Core Services. This Network manages business models for selling the use or purchase of decentralized Resources within a trustless environment. Nodes monitor the existence and status of Resources and verify their use or transfer to other parties.

The entire structure is designed to support decentralized commerce driven by economic activity generated from a decentralized inventory of Resources. The network's goal is to enable anyone, anywhere to monetize anything that can be monitored and measured by a Smart Meter run by a Worker Node. This is achieved using trustless technologies such as DLTs, cryptographic proofs, secure hardware and software. The Network employs a range of risk management techniques to reduce the risk of economic loss by unauthorized access, use or fraud.

At its core, the Network's approach to managing risk involves the use of highly-controlled, verified hardware and software to create a highly secure backbone. This high security framework enables existing communications, hardware infrastructure and software to operate in a more secure and lower risk way. It is further enhanced by testing and verifying an increasing set of decentralized suppliers of enhanced security communications, hardware and software.

The result is a decentralized edge-based Network with a high trust, low risk, high security framework that can be used in a trustless environment. This framework is designed to be difficult and costly for even sophisticated nation state actors to compromise. Additionally, It is designed to allow augmentation by any qualified supplier that passes verifications and audits of enhanced security hardware and software for use in conjunction with the high security environments at a lower cost.

Finally, the Network can be used to convert existing technology and software environments into Worker Nodes that mine by managing the use, sale, and transfer of Resources.

Resources

A Resource in the Network is anything that has economic value. The whole purpose of the Network is to manage its Resources to create the greatest amount of economic value for the Network's Participants, Operators and the Resource owners. This is accomplished by enabling as many customers to use as many Resources as possible to maximize economic activity that mines Network Assets.

Resources are the things measured and monitored by Smart Meters running on Worker Nodes. A Resource can be anything of economic value that has its use, sale or transfer measured by a Smart Meter. Resources can be thought of as the Network's inventory of IP, assets, services or goods for which the Network can:

- Rent the Right of Use for a period of time,
- Sell the Right of Ownership, or
- Transfer the Right of Possession.

Mining occurs if the revenue results in the purchase of CROP. The Resource is used to mine CNDT. The Resource Owner determines what percentage if any of the transaction's value goes to the purchase of CROP. However, every transaction on the Network must use CNDT as its settlement currency – however, this can be made entirely invisible to the customer through Gateways.

Growing the Network requires more and more Resources that produce CROP to enable Parties to mine both CNDT. CNDT is the Network currency.

These Resources can be any form of IP, asset, service or good that generates revenue that produces CROP, not just hardware or software. For example, they can be a service delivered by a human being, such as, a meal at a restaurant using a Smart Meter running on their point of sale device which acts as a Worker Node.

A Resource could be a Worker Node itself running the Worker Node OS selling VMs running containers, or providing access to content, files, records or objects stored on a Worker Node. Resources can be processes, CPUs, GPUs, bandwidth, memory, storage, AIs, IP, assets of any kind, or human-based services or goods. Again, it's not just hardware, anything that can be monitored or measured by a Smart Meter running on a Worker Node can be a Resource.

Regardless of Resource type, its use or transfer is controlled by a Core Security Node. One Core Security Node can control millions of Resources, or only a few, depending on the processing capacity of the Core Security Node and the transaction volume related to the Resource. The Network is designed to protect its Resources from unauthorized access, use, or monitoring by malicious actors. It enables its users to determine the level of security, risk, and trust they desire – and then ensures this desire is enforced.

Security, Risk and Trust

A key goal of the Network is to reduce the risk of economic loss from malicious actors and error while still enabling Resources and Nodes to operate on the edge in insecure environments. This goal is not some utopian, risk, fraud or error free environment that would make a platform uneconomical and overly frustrating to use. Instead, the goal is to limit unauthorized access, use, fraud, or error risk to economically acceptable levels as determined by each Participant. This is why hardware Nodes are divided into four Trust Levels, which indicate the associated risk in their use and corresponding security.

It is important to remember that Nodes can monitor human actors, IoT devices, etc. not just servers.

Trusted Hardware

The Trust Levels for hardware Nodes are defined as follows:

- **Low Trust** – Nodes appropriate for use only when there is virtually no value should the device be compromised - or gaining access to or changing the information it contains or produces. Shared public information that can be easily regenerated is a good example. Any hardware system can be considered a Low Trust Node. In fact, all non-verified Nodes in the Network are considered Low Trust Nodes until proven differently. This means that any device already owned or in use by anyone on the internet can be considered and used as a Low Trust Node. The Conduit infrastructure Ecosystem websites and apps do not offer any pre-configured Low Trust Nodes as their use is not encouraged by the Network. However, every piece of hardware connected to the internet today, unless certified to a higher standard, every cloud computing environment is considered Low Trust.

- **Standard Trust** – Nodes appropriate for use where there is low value to someone gaining unauthorized access, or for use where there may be economic loss, but which would not be significant – either in individual cases or the aggregate. Standard Trust Nodes may be considered Enhanced Nodes when they exist in environments that have high physical and connectivity protection. For example, in secure data centers or in private networks not connected to the internet. Standard Nodes can be supplied by many commodity hardware providers. Even legacy hardware that Network Participants already own may qualify for use as a Standard Node. Standard Nodes can be acquired directly from their suppliers and configured to operate within the Network by installing a Worker Node OS by purchasing a Node0 License. Also, a limited list of pre-configured Standard Nodes are available for purchase via the Conduit infrastructure Ecosystem websites and apps. These come with the Worker Node OS preinstalled and a Node0 license.

- **Enhanced Trust** – Nodes that represent a compromise between Standard Trust and High Trust that attempt to find the sweet spot between cost and the friction of use versus the skill or economic cost of breaching security or violating trust. Enhanced Trust Nodes are only available from a list of qualifying hardware device manufacturers from vetted third-parties. Enhanced Trust Nodes can be purchased directly from their suppliers, and can be configured to operate within the Network by buying a Node0 License – or purchased pre-configured through the Conduit infrastructure Ecosystem, which comes with the Worker Node OS preinstalled and a Node0 license.

- **High Trust** – Nodes that are appropriate for use in the most demanding trustless security environments, including critical banking, nation-state, and utilities infrastructure. These Nodes can only be purchased through licensed Syndicates (a Network version of a DAO) within the infrastructure Ecosystem. These Syndicates must demonstrate that they maintain a fully audited supply chain that provides full provenance for all components. All components deemed to pose a quantifiable risk must also come from Members of a licensed Syndicate within the infrastructure Ecosystem. All hardware, OS and software for High Trust Nodes are designed by Conduit, and are only manufactured by licensed Parties who use approved suppliers for components. Software components can only be created and modified by licensed Parties and must be audited by licensed Parties. All hardware for High Trust Nodes that run Core Services must be NIST rated to comply with the FIPS 140-2 (level 3) standards or higher.

  The entire supply chain for High Trust Nodes must ensure provenance and auditable history of each component. Any party who wishes to participate in building components for High Trust Nodes must go through a rigorous training process, risk assessment and submit to regular audit processes, as well as agreeing to join a Syndicate that places the right to all IP used within a Network trust. Therefore, High Trust Nodes for use in the Network are only available through the Conduit infrastructure Ecosystem and must be purchased through Network websites or Apps.

The Worker Node OS can be run on any of the four Trust Levels of hardware. However, Resource owners and Users determine the level of hardware they want their Resource's Smart Meter and associated transactional data held on. For example, a business might only want to use an AI running on their own High Trust Nodes to protect the sovereignty of their data.

A Core Security Node can only be run on High Trust hardware.

Trusted Software

Just as hardware has four Trust Levels software also has four Trust Levels. The difference is that software includes operating systems, drivers, libraries, packages, services, applications and cloud services. The Network runs a Trusted Store that operates like an App store on a digital device. Software and code library creators can submit their code for audit and review by a decentralized set of Auditors who will review their code and sets its Trust Level before allowing it to be released to the Trusted Store.

The Trust Level of a Worker Node is set by the lowest Trust Level of the hardware or code running on that hardware. For example, running a lower Trust Level of code on a High Trust Node downgrades the High Trust Node to the Trust Level of code. The same is true of the reverse. Running a higher Trust Level of code on a lower Trust Level of hardware results in a lower level of trust for the code.

The Trust Levels for software running on Nodes is defined as follows:

- **Low Trust** – Code that is appropriate only when there is virtually no value to compromising the software or data it stores. Many public information websites are an example. Any piece of code can be considered a Low Trust Code. Therefore, any Worker Node can run any piece of code but the Worker Node Trust Level will be downgraded to Low Trust.

- **Standard Trust** – Code that is generally designed to a common standard of security in the market. The code can use its own authentication and authorization services, but must utilize Network Frameworks and Core Services for billing, data/file access, settlement and payment.

- **Enhanced Trust** – Code that is generally designed to a common standard of security in the market. Additionally, the code must use the Network authentication and authorization services, and also respect Party and Agent definitions within the Network. All Network-defined problem domain specific languages can be used to create Enhanced Trust code. Enhanced Trust Code must use Network Frameworks and Core Services such as; data storage, replication, messaging, events, predicates, billing, accounting, settlement, payment, etc. where applicable. Enhanced Trust Code must be audited by a licensed Network party before being submitted to the Trusted Store.

- **High Trust** – Code that is generally designed, created and audited by licensed Network parties. Additionally, non-licensed parties can submit code written in one of the Networks problem domain specific languages to be compiled or interpreted by Network compilers or interpreters. All High Trust Code must be audited using Network Licensed Security Auditors, and is only distributed, installed and verified by the Core Security Nodes. Only High Trust Code can run on

High Trust Worker Nodes or Core Security Nodes. Only High Trust Code can be installed or executed on a Core Security Node.

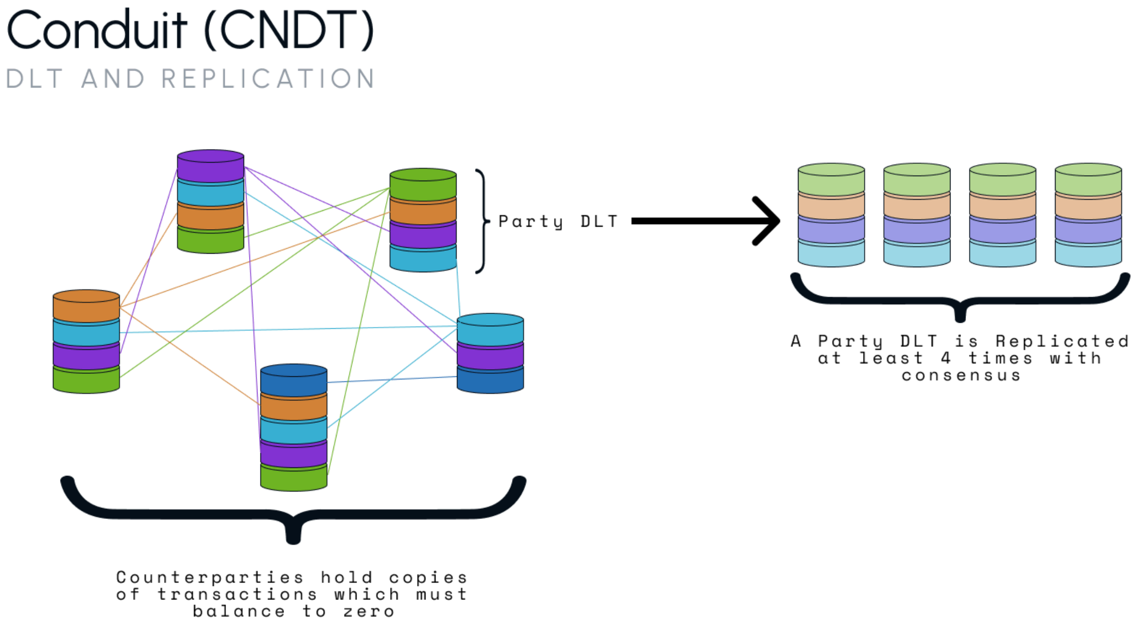
Trust Bridges and Gateways are a special class of High Trust Code that use Network protocols and standardized frameworks to enable their creation by developers participating in Conduit Labs. Conduit Labs offers incubation and design assistance for developers wanting to build and monetize Trust Bridges and Gateways. In these cases the developers do not need to be licensed but work with a licensed mentor who helps them architect and design their code. All wallet Apps must be High Trust code and all Predicates are High Trust Code.

Mesh of Immutable Event Store

In order to have infinite scalability, high performance, and also to conserve Core Security Node CPU, bandwidth and storage, the Network does not use a blockchain. Blockchains require a majority of nodes to reach consensus before a block can be validated, which requires massive replication of the block. Instead, the Network leverages the strength of its hardware level security to approach the problem differently. It uses a mesh of DLTs with each Party having their own DLT, and where multiple DLTs run on the same Core Security Node, using a hashed immutable event store.

Event stores are some of the highest performing data storage structures, and are used in many of the world's most demanding transaction processing systems. By design, event stores only update or depreciate and don't modify or delete, therefore they are immutable by design. Adding hashes to an events store enables it to operate like a Merkle tree or graph. By interconnecting all counterparties in a transaction, it is possible to create a DLT with each counterparty having a copy of the same data and its hash, but each Party's total hash is different except on replicated cluster Nodes.

The Network does not use a block, but a variable-sized transaction, which must be confirmed by all counter-parties and a majority of each counterparties' clusters. This enables a highly parallelized transaction and consensus process, which avoids “hot spots”, and has near linear scalability to the number of Core Security Nodes in the Network. It can use a combination of a standard multi-phase database commit along with a replication hash for consensus for the set of all Party data. The interesting thing about this approach is that it can be implemented in almost any database technology. This means that over time the Network should be able to create its own versions of cloud database services that use this same technique for SQL, Graph and Document database structures.


Conduit (CNDT)
DLT AND REPLICATION
Party DLT
A Party DLT is Replicated at least 4 times with consensus
Counterparties hold copies of transactions which must balance to zero

Therefore, trust does not have to be created by staking of massively expensive proof of work to be trusted by the Network hardware layer and OS. Instead of relying on concurrent copies of data stored across the network, the Network uses a special form of caching. This allows the master copies of a Party's data to move to Nodes where it is most used, or to where the Party explicitly wants their data stored. This results in data that can dynamically migrate to where it will provide the best performance to the Party and its common counterparties, and improves overall Network performance.

Business Model

The Conduit Network is designed to provide foundational infrastructure for the 4th industrial revolution. The emergence of the “digital society” creates an opportunity for a new business model to emerge: “Society as a Service.” Society as a Service enables individuals and businesses to choose something they could not easily do before – the society they want to operate within. The digital world is beginning to map everything in the physical world into an environment that is increasingly more accurate and real time. This is still nascent, but it is happening at an incredibly fast rate that is accelerating. This means that in many areas of the world, such as emerging nations, where corruption and fraud with the associated increased risks, it is now possible to create business models that force lower corruption levels and related fraud.

This, along with the digital society’s ability to circumvent the historic reliance on local civil society to ensure fairness and provide dispute resolution, digitally creates a massive arbitrage between physical world risk and digital society risk. The advent of new digital technologies such as AI, DLT, drones, IoT, machine vision and satellites to provide near real time monitoring of the physical world to ensure accuracy, means the reliance on individuals to ensure accuracy is diminishing.

The effect of this dynamic is another new type of business model known as “Outcome as a Service.” With respect to establishing a new internet, it is essential for the business model to be owned by all of its stakeholders; the customers, investors, suppliers, nonprofits and governments that participate. The value of a new internet that can support this business model is so great, it could have an even greater impact on global society than the four industrial revolutions. This business model can dwarf that of Amazon or of any business model in history, which is both a great opportunity and a great risk if not initially founded for the benefit of all of its citizens.

The reason being that the business model can be used to align all of its stakeholders economically with a single outcome, the growth of mutualized net worth, and reduction of mutual cost. This can either lead to freedom, or if established in the wrong ways, it can lead to a new form of extraction. Therefore, the opportunity is much like the discovery of the new world centuries ago. If the digital society simply serves the current version of the colonial masters, we will get the same results recorded in history with European powers extracting the value of the new world for their sole benefit. However, if we form a digital society as a new society wherein the principles of self-governance, along with a set of rights and obligations that all parties must live by, we get the opportunity to correct and learn from mistakes in the past.

This can be achieved with a highly decentralized model of governance where the value the Network creates is owned not by a government, but by its citizens. One where each individual is literally an owner of the society in which they live. Like an ESOP, but for a whole society.

However, if a digital society becomes as large as a major economy, and is controlled by governments or by major corporations instead of its Participants, it could become the equivalent of a dictatorship or totalitarian regime of extraordinary power. This cannot be allowed because it would create a great risk to individual freedoms and potentially lead to a new form of enslavement. Even if it were started by benevolent actors that acted as a good monarch, the risk that the next generation would not be as benevolent is simply too high. The beauty of a digital society running on a new decentralized version of the internet is that if properly designed, it can enable the freedom to either voluntarily participate, or not, which is the indicator it is based upon freedom of will instead of lies, coercion or manipulation – control.

To support this, the Network is designed with an entire economic reward system built into its fabric. This system is designed to reward the behaviors that are needed to create a new decentralized internet. It is made up of key, platform-defined roles that ensure proper governance, and reward distribution to those that create the value of this new internet - not simply a group of founders and investors.

See white paper on Conduit Network Reward System – Mining, Network Pools and Distribution

The Economy

The root entity in the Network is the Network’s economy, which is the central reward system hosted on the Network. The Network is designed to support any number of economies architecturally, but is only being released at this time with one for real commerce and multiple others for testing and development.

The Economy defines the rules by which everything else is governed. This is done through Authority Rights, which are legal rights of authority, not security settings. These Authority Rights come from an Accord or what some might call a Constitution.

The Economy is made up of special classes of Party which can be an Ecosystem, Syndicate, DAO, User, LPEntity, Citizen or LPMember. Each Party can have a parent, which is ultimately the Economy. The Economy contains any number of Ecosystems which can be thought of as legal jurisdictions, each with its own set of governance, rules, policies and membership.

Ecosystems

Ecosystems are formed by the Network community. However, the Network has three Ecosystems it formed as an example:

1. A Network infrastructure Ecosystem, which provides all hardware and software for the Network through licensed Participants.
2. A financial services Ecosystem, that is comprised of financial institutions that are also building Gateways.
3. The Conduit Labs Ecosystem for organizations and individuals building Network Apps and Services, Gateways, Smart Meters and Trust Bridges.

Ecosystems contain members (Citizens or LPMembers) and Syndicates. The Ecosystems are effectively DAOs of DAOs. There are two types of Ecosystems:

- **Wrapped** – Wrapped Ecosystems have a legal entity wrapper to establish the ability to contract with the real world and set the jurisdiction of standing in a legal dispute. This means that Wrapped Ecosystems can ensure proper tax treatment of sales tax, income tax and proper accounting or regulatory reporting. In addition, it ensures that legal disputes occur in the legal jurisdiction of choice, not every legal jurisdiction that wants to claim standing. Ecosystems are licensed entities that must be the equivalent of a non-stock legal entity so that no value is leaked away from shareholders. Wrapped Ecosystems are made up of Members and Syndicates.
- **Unwrapped** – Unwrapped Ecosystems are simply a DAO of DAOs. With the governance of the root DAO being applied to all member DAOs or Members.

The rule, policies and governance at Ecosystem level apply to all Members and DOAs or Syndicates within the Ecosystem. Participation in an Ecosystem is voluntary and any Participant can be a Member of as many Ecosystems as they wish.

There are currently four types of Ecosystems:

1. **Industry** – This is an Ecosystem focused on an industry such as the agriculture, financial services or media Ecosystems, which are already forming on the Network. The financial services Ecosystem, which is a Wrapped Ecosystem, is an example of this type of Ecosystem.
2. **People Group** – This is an Ecosystem that is focused on one or more people groups such as the diaspora from Zimbabwe, African Americans or the Zulu's.

3. **Region** – This is an Ecosystem that is focused on a geographic region such as a country, city or area.
4. **Value Chain** – This is an Ecosystem that is focused on a value chain such as organizations that make the hardware components and software for the Network itself. The infrastructure Ecosystem is an example of this type of Ecosystem.

Ecosystem also can make use of Economy-wide shared service operators for things such as legal, accounting, marketing, risk management, security and other functions. These functions are provided by independent but Network Licensed Roles that prove they have the skills and reputation to be trusted. The Parties that fill Licensed Roles must post a bond in the form of a Proof of Stake in Network assets.

Syndicates

Syndicates are DAOs inside of a Wrapped Ecosystem which means they function like a subcontractor in an Ecosystem, but which are not legal entities themselves, rather a consortium governed by the Syndicate Governance under the Ecosystem Governance. There are many tax and legal advantages to operating as a Syndicate inside of a Wrapped Ecosystem such as the ability to trade with other Syndicates without sales or income tax in many cases.

DAOs

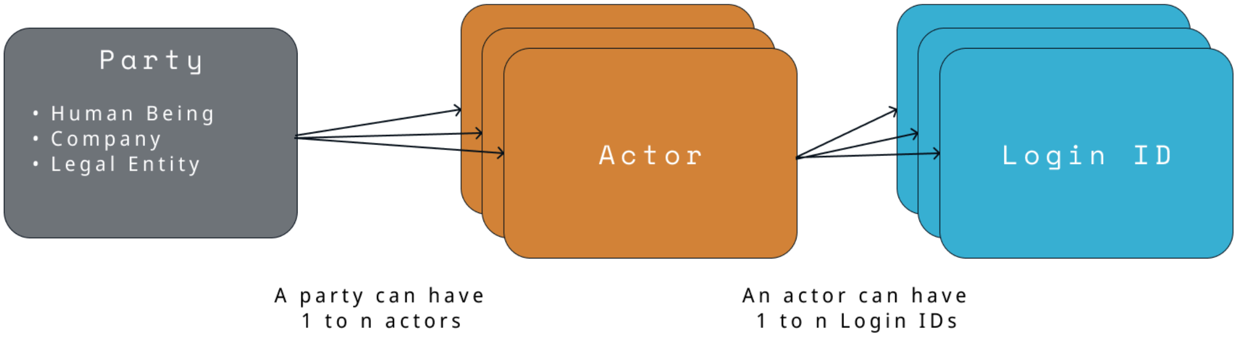
DAOs are the equivalent of Syndicates but in Unwrapped Ecosystems. DAOs must handle all of their own legal, accounting and tax as there is no standing for establishing a legal jurisdiction. Everything a Syndicate can be configured to do related to governance and automatic distribution of assets can be achieved by a DAO as it has its own root Accounting Entity.

Parties

The root identity concept is a Party. A party can be a Legal Entity like a company, a Human Being or a Logical Entity like a DAO or Syndicate. Parties can be Citizens or registered Legal Entities who have joined the Network as a Member or they can be simply Users or organizations who are conducting commerce within the Economy, but have not actually joined. Actors take action on behalf of a Party, and identify themselves with some kind of credential known as a Login Id. When a Party is acting on its own behalf the Actor is Self.

Conduit (CNDT)

PARTY, ACTOR, LOGIN ID



A Party can have zero or more Actors that initiate action each with one or more Login Ids which represent a method for the User to be authenticated through a technology. These login methods have varied degrees of trust, some being weak and others being very strong methods of authentication. Therefore, when we say a User is authenticated with a particular Login Id, the level of trust associated with this authentication may vary depending on the method.

There are four types of Parties that represent Individuals and Organizations. The primary difference between them is the level of trust, their participation in the Network's rewards program, and governance. The level of trust controls the roles they can play in the Network. Users and Organizations can use the Network without participating in a KYC process or operating under the Network's governance and rewards system. Participation in the Network rewards requires the agreement to operate under Network governance, such as passing KYC and rules which are designed to prevent bad actors from harming Members.

To keep the Network decentralized, it uses KYC/KYB and licensing of Individuals and Organizations who want to play roles that require an enhanced level of trust. The Network has five levels of trust for both Individuals and Organizations that are grouped into two levels that represent a threshold of trust vs anonymity:

- **Network Users** – There are two levels of trust within the User category, No Trust and Low Trust.
    - **No Trust** – means that only a phone number, email address or individual who is a Enhanced Trust Citizen has been used to verify the Party.

- **Low Trust** – means that a minimal level of KYC/KYB has been performed that is appropriate for their location and economic activity.

Network Users are Parties that simply want to use the Network as a Supplier or Customer and do not wish to participate in any active way. Network Users are passive participants in the Network. There are two types of Network Users:

- **Users** – are individuals who are Non-Members and have at most lightweight KYC requirements to prove emails or phone numbers are indeed controlled by them. Users are relatively anonymous but can't serve in Network Roles that require a level of trust or bonding. Users can buy and sell, use and transfer Resources on the Network but have limits to the size and amount of the economic value they can transfer to others.

- **LPEntities** – are companies, organizations or governmental entities which are not Human Beings and have at most lightweight KYB requirements. LPEntities can buy and sell, use and transfer Resources on the Network, but have limits to the size and amount of the economic value they can transfer to others.

- **Network Members** – There are three levels of trust within the Member category, Standard Trust, Enhanced Trust, and High Trust.

- **Standard Trust** – is equivalent to enhanced KYC/KYB in many financial institutions, but is also adapted to work for the unbanked and those living in poverty.

- **Enhanced Trust** – requires the posting of a Network Bond (similar to a proof of stake) and is the minimum level of trust needed to obtain a Network License or act as an Actor for a Network licensed LPMember.

- **High Trust** – is the highest level of trusted Party, and requires multiple biometric proofs, the ownership of at least one Core Security Node, and the posting of a Network Bond. They are able to serve in any Network Role, obtain a Network License, or act as an Actor for a Network licensed LPMember. Only High Trust Citizens can participate in any form of Network level governance.

KYC/KYB can be performed by anyone holding a license to act as an Administrator within the Network. Network Members are active participants in the Network. There are two types of Network Members:

- Citizens – are individuals who are Members of the Network's digital society, go through enhanced to substantial KYC requirements, and potentially the establishment of enhanced authentication proof. This enables them to recover their own lost keys, transfer significant value, play Network Roles, and participate in Network rewards. These levels are designed to protect people from identity theft, and to ensure that people don't have more than one Citizen identity on the Network.

- LPMembers – are individuals who are Members and provide moderate to substantial KYB information requirements that enable additional levels of authentication proof. This requires the provision of the Ultimate Beneficial Owner (UBO) information for individuals within all parties that control 10% or more of the organization. They can assign Actors and are able to recover their own lost keys or accounts and transfer significant value.

Actors

Parties can have any number of Actors, which can also represent the level of Authentication for a Party. This can include requirements that specific devices, or Core Security Nodes be used to authenticate. A Party can have multiple actors act on behalf of themselves with Authority Rights being defined in a Mandate. Mandates allow other parties or various logon identities for a single Party to have different levels and types of Authority to act on the behalf of a Party.

Accounting Entities

Accounting Entities collect all accounting related information for Parties. This includes each Party's Wallet which is stored on their own DLT within multiple Core Security Nodes. Wallets are made up of accounts for a specific, fungible asset;s balance and the correlated transactions – similar to a bank account or investment account. Wallet accounts must also be connected to either a Registry or Treasury account.

Every Party has an Accounting Entity known as the Root Accounting Entity that acts as the master rollup Accounting Entity for the Party. Parties can have any number of Accounting Entities, which can hold Wallets and accounting information for various purposes – each of which can have Mandates for other Actors to view or authorize funds from the Accounting Entity Wallets.

Network Fees

The Conduit Network consists of decentralized Worker Nodes that must work together with Core Security Nodes to mine through economic transactions.

All economic transactions can have up to three types of fees. A fee for the:

- **Network** – this fee is set by the Network governance and is currently a minimum of 10 basis points (0.1%) of the economic value being exchanged with a cap of $250 per transaction. This fee is equally shared between up to 3 Core Security Nodes involved in a transaction. If a Party desires to use more Core Security Nodes to increase the validators, or includes more counterparties that increases the number of Core Security Nodes used, the fee goes up proportionally. This fee goes to the Parties that own the Core Security Nodes used to process the transaction, which may be a Syndicate (or DAO). At least two Core Security Nodes must verify a transaction before it can be considered complete. The number is determined by the value of the transaction, the risk tolerance of the counter-parties with each other, and the number of counterparties. 100% of this fee is converted to CROP to enable mining.
- **Operator Fee** – this fee can either be set by the Worker Node owner or can be set by the market. This fee covers the cost of the Worker Node, communications bandwidth, depreciation, physical space and power. The higher the Trust Level of the Worker Node the higher the fee. The Network publishes a market price for Worker Node usage so that Worker Node owners know what buyers are paying in the market. Core Security Nodes manage capacity and the use of the Worker Nodes based upon the pricing the respective Worker Node's owner desires for its

use. By default, a Worker Node is configured to use the market price. The amount of this fee that is contributed to CROP is set by the Worker Node owner, but must be at least 10%.

- **Resource Owner** – This fee is set by the Resource owner. Resource owners can set their own fees for their Resource's use, purchase, or transfer. One Resource owner may need a Resource from another Resource owner to offer services to a customer. Therefore, inside of the transaction, the fee the user pays may ultimately result in fees being distributed to multiple Resource owners. For example, in an Airbnb type of marketplace app, the user rents a house through the app which charges the user a fee for the house. But the app must pay the owner of the house, which is a Resource registered by the owner of the property. The app may also pay for settlement services for a Resource that processes payment through a credit card, and so on. The amount of this fee that is contributed to CROP is set by the Resource owner, but must be at least 10%.

Except for the Network fee itself, all others may be established by the owner of the Worker Node or Resource. This means the owner of the software, hardware, AI or asset can set the fees they want to receive for its use. On the other hand, for many commodity items or services, the Network publishes recommended pricing to provide guidance to Participants.

Community Developed Apps and Services

The Network is designed to empower a development community to create Apps and Services, Gateways, Trust Bridges and Smart Meters. The Conduit Labs Ecosystem is designed to provide training, technical support, marketing and in some cases grants to entities who wish to develop on the Network and monetize their components. Developers of any community component may set the fees they want to charge for their components' use, but at least 10% must be used to purchase CROP to enable mining.

Apps and Services

Unlike typical L1 blockchains, the Conduit Network can work with Apps in both the Web2 and Web3 architectures as well as Web2 server-based microservices. This is possible because the hardware and software Trust Level is not affected by the party that physically has possession of the device on which the code executes.

In normal Web2 environments, only the software executing on hardware in a trusted data center that restricts physical access and is operated by a trusted party can be considered as trusted. In the Network, this is no longer true because the only thing that must be trusted is the code itself, which can be audited and limited to restrict access to the outside world, and forced to store data in secure locations. For this reason, only Enhanced Trust Nodes or High Trust Nodes should be used for Web2 services and Apps.

The entire network shares a common authentication and authorization system maintained by the Core Security Nodes, and is respected by Worker Nodes. Which apps and their backend services they are allowed to use or connect with, what they can see, and where they can write data, can be enforced Network-wide.

Another implication of the Network's architecture is that any existing app, web app, web service or microservice can be ported to the Network and used to mine. This includes open source projects which can use the mining as a means of supporting the developers who create and maintain the open source projects. To facilitate this, the Network supports an Open Source mining pool that receives 10% of all tokens mined to provide grants to sustain Open Source projects that support the Network.

Many open source projects are created and maintained as passion projects by developers who are some of the best developers in their areas of expertise on the Internet today. To create a decentralized internet, the Conduit Network needs more and better open source projects. This requires trusted code, therefore anyone can submit an app or back end service through Conduit Labs for a decentralized audit of their code to obtain a Trust Level rating.

Gateways

There are two types of Gateways, financial and informational. Financial Gateways enable anyone to use their accounting entity and wallets to connect to one or more financial services organizations. Informational Gateways enable the Network to connect to external information sharing or message systems.

To enable the widest number of payment and settlement options, the Network allows developers and financial institutions to build payment and settlement Gateways. Gateways can provide autonomous exchange, payment and settlement services to the Network for anything from cellular airtime, banks, card networks, exchanges, gift cards, payment rails, stocks, bonds, commodities, etc.

Developers of Gateways can charge fees on their Gateway's use. This allows a community of fintech companies with existing technology that accesses financial services to create a single Gateway that can be used by any Network user, application or service. In addition, the Network itself provides several Gateways to provide payment rails to US ACH and Single Euro Payments Area (SEPA) payments plus currency conversion, cryptocurrency exchanges and Decentralized Exchanges (DEXs).

The Network provides a standard framework for developers of Gateways. For financial services Gateways, the Network provides an Ecosystem for financial services providers who wish to promote the use of the Network for access to their products and services. Gateways can only operate on High Trust Worker Nodes and must be High Trust Code audited by a Network licensed auditor.

Trust Bridges

Because of the Network's architecture, blockchain and token Trust Bridges can be securely built and operated on High Trust Nodes. This allows any existing token to be moved from its native blockchain to the Network, or from the Network to another integrated blockchain. Once a Trust Bridge to and from a chain is built to support one or more of the specific types of Trust Bridges, it can be used for any of that chain's assets of the same type. One Trust Bridge can therefore support any number of tokens for a specific chain.

The Network natively supports several types of Trust Bridges:

- **Tokenization on Demand** – allows conventional assets to become tokens on a target blockchain on demand, within the verification speed of the chain. The Network supports both tokenized and non-tokenized assets for backward compatibility and easy integration. In addition, in many legal environments, it is desirable to be able to work with non-tokenized versions of the asset where transfers occur via legal documentation and legacy processes. In these cases a non-tokenized version of the asset class can be used to seamlessly move between legacy environments and Web3 environments on demand.
- **De-tokenization on Demand** – allows parties in possession of a tokenized asset to convert it back to a conventional asset with both a digital and paper (PDF) record. This allows existing regulatory parties in any jurisdiction to work with digital assets.
- **Native to Chain** – any Network asset can be materialized as a token on any number of blockchains. The Network's CNDT token is an example of this functionality.
- **Port to Native** – many existing blockchain assets can be ported into native Network assets by their projects using their existing tokens as if they were tokenized on demand. They get all of the added benefits of being able to separate Rights and Obligations, faster settlements and lower transaction costs or to participate in Network mining. No other DLT or blockchain can separate the property rights of Ownership, Possession, Use and Destruction. However, because the Conduit Network can, it solves many issues pertaining to the custody of the asset. When the token for an asset is imported to the Network, it is effectively burned on its original chain, but can still exist there when so desired or is necessary.
- **Use as Native** – blockchain tokens can be moved from their native blockchain's to the Network so that it can be used within the Network to obtain the added benefits of separation of Rights and Obligations, built in hardware backed up wallets, faster settlements and lower transaction fees or to participate in Network mining.
- **Chain to Chain** – allows a token to be moved from one blockchain through the Network to another blockchain.

All Trust Bridges that move tokens from another chain to Network native digital assets can also enable the separating of Property Rights on the asset. This enables the Rights of Ownership, Right of Possession and Right of Use to be separated and held by different parties. It also enables these Rights to be tokenized as different tokens. This solves the problem of custody of digital assets, and enables many interesting behaviors, which would otherwise be too complex to create via smart contracts because the behavior would have to be natively built into the token via its smart contract.

For example, placing the Right of Use in a 30 month lockup where the Rights of Ownership can still be traded, even though the asset itself can't be used. This creates the lockup effect of a multi-sig wallet, but allows the asset to still be traded keeping the lockup itself preserved so it can't be listed. It also allows transferring the Right of Possession to a custodial account that can't sell or use the token because the custodian doesn't have the Rights of Ownership or Right of Use.

Trust Bridges can only operate on Core Security Nodes, and must be High Trust Code audited by a Network licensed auditor.

Smart Meters, Predicates and Billing

Smart Meters are oracles that function as a mix between smart contracts and oracles on traditional blockchains. Smart Meters are used to detect and measure off Network DLT events. They run in the OS layer of a Worker Node, which is the highest trust ring on the device. Smart Meters monitor or sample data streams of events, or make measurements storing changes in a Network Temporal Ledger. For example, on a Worker Node a Smart Meter monitors the use of memory, CPU, storage and bandwidth.

Smart Meters support a predicate language that is used to define significant events and measurements that are communicated via a cryptographic proof to Network Message Queues and Petri Nets. This language allows developers to define when a:

- significant event occurs within a workflow that will trigger a state transition,
- notification event occurs for human or machine notification,
- periodic event occurs with the measurements or metrics related to resource for that period, or
- heartbeat that represents a time interval passing without a significant event occurring.

Predicates support the ability to transfer information about an event or measurement to Message Queue subscribers in the form of a Predicate Proof. A Predicate Proof supports both zero knowledge proofs or transparent information accessible by anyone with Authority to access the Predicate Proof.

Smart Meters

Smart Meters perform two functions:

- the creation of Predicate Proofs upon a Predicate detecting an significant event, and
- providing Billing information for use, sale or transfer of a Resource the Smart Meter monitors or measures to a Core Security Node to calculate the charge and do the Billing and Settlement.

All Smart Meters must implement these two functions.

Smart Meters can deal with five types of events:

- **Calendar** – events based on time of day, date/time, day in a period, holiday, etc.,
- **Duration** – based events related to elapse time; minutes, hours, days, etc.,
- **Message** – based on the call of an API, receipt of a message or the addition, change or deleting of a file,
- **Polling** – the periodic call of an API, script, URI or process that provides a return, and
- **Signal** – based events such as a call to API supported by the specific type of Smart Meter.

Smart Meters are written to work for a specific type of Resource or class of Resource. They can be built to work with special devices or to support a particular system. For example, IoT temperature devices, vehicle operations sensors, point of sale devices, credit card machines, bank account balances for a specific bank, inventory control systems, etc. There are theoretically an infinite number of Smart Meters that can be created because there are an infinite number of Resources that could be controlled by the Network.

The Network provides a set of Smart Meters for Worker Nodes and some others for common use cases (primarily as examples). However, Smart Meters are like oracles and smart contracts on blockchains, which are intended to be created by the Network's community. Therefore, Smart Meter creators can participate in the fees and mining that occurs as part of the transactions their Predicates are used to initiate. This means that developers who create Smart Meters can earn an income from the use, sale or transfer of monitored Resources managed by a Worker Nodes that use their Smart Meters.

Smart Meters must publish a special message to their Message Queue called a heartbeat. Heartbeats are periodic messages used to indicate the Smart Meter is running fine but has nothing significant to report. All Smart Meters must make available a common set of JSON objects required for the session, Resource, and environment to enable a Predicate to function. Creators of a Smart Meter may define enhancements to the global schema and taxonomy when they are needed to support Predicates or Billing for the type of Resources the Smart Meter manages. Therefore, Smart Meter creators may add additional information to the User's session, Resource, and environment objects for this purpose.

Smart Meters must be audited in order to be certified for a Trust Level higher than Low Trust or to be executed on Worker Nodes with a Trust Level higher than Low Trust. A Resource Owner may specify any Trust Level for the Smart Meter monitoring its Resources. The Network recommends the use of Enhanced Trust or High Trust Meters running on Enhanced Trust or High Trust Nodes for risk reasons. Users who are uncomfortable with a Resource Owner's specification of Trust Level may opt for a higher Trust Level for the Worker Nodes they utilize. This way the market decides on the Trust Level needed for the Resources the market uses.

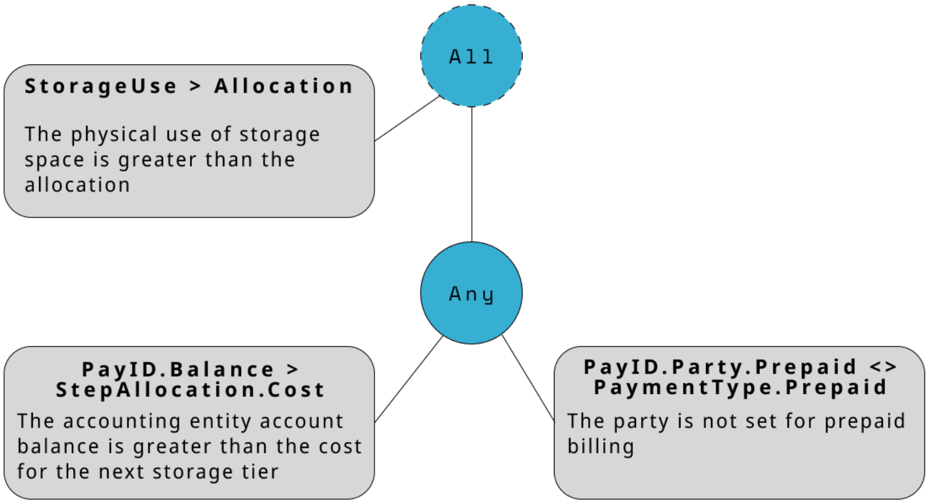
All access to a Resource must be approved through a Smart Meter. This enables the Smart Meter to determine if payment for the Resource has already occurred or needs to occur. This enables the support of a real-time Billing process prior to enabling access. Real time Billing processes occur prior to the access being granted. All Billing processes are settled in CNDT. Smart Meters can grant access for a session, a duration or a period of time. Billing that supports near time and periodic billing are also supported by the Network.

Predicates

Predicates are made of boolean statements that use values stated in an object graph the Smart Meter exposes to its Predicates at execution of an evaluation of the Predicate. All Smart Meters expose a

Conduit (CNDT)

PREDICATE EXAMPLE


All
StorageUse > Allocation
The physical use of storage space is greater than the allocation
Any
PayID.Balance > StepAllocation.Cost
The accounting entity account balance is greater than the cost for the next storage tier
PayID.Party.Prepaid <> PaymentType.Prepaid
The party is not set for prepaid billing

graph of standard attributes, along with an optional set of Smart Meter specific values for Predicates that are Smart Meter specific. Predicates allow Parties with authorization in the Network to monitor Resources for events, and measure the Resource's environment in ways supported by the Smart Meter at the point of observation. This occurs without leaking information or exposing information because they execute on the Worker Node running the Smart Meter.

There are three default categories of Predicates that must be defined for all Smart Meters: the Predicates for use, purchase or transfer events. At least one Predicate that covers all cases for each category must be defined by the Smart Meter for each class of Resource it manages.

Predicates can be expressed in both a language or a graphical form. They represent a formal means of describing what triggers an event. When expressed graphically, the dotted lines around operators indicate that the variables used in the evaluations are published with the proof. When solid lines are used around the operator it means the variable values are zero knowledge. Regardless of which type, the Predicate Proof is signed by the Smart Meter and Worker Node, which can be validated by a Core Security Node for the Worker Node.

Predicates use a domain specific scripting language that is used by all Smart Meters. This can support multiple Predicate scripts being evaluated in parallel on the same Resource. Information collected by Predicates are stored in immutable temporal ledgers on the Worker Node running the Smart Meters for the Resource. Predicate Proofs are authenticated and stored on the Services Nodes for the Worker Node.

Predicate Proofs and Message Queues

Predicates generate a special type of cryptographic proof called Predicate Proofs. These Predicate Proofs are used to prove an event occurred. Once validated, Predicate Proofs are placed in a Core Security Node Message Queue, and are used to inform subscribers about events in which they are interested.

Predicate Proofs can be used to indicate when:

- the use of a Resource reaches a billable event,
- a sales event occurs, or
- when a transfer event happens.

Interested Parties with proper Authority can subscribe to specific events via a Core Security Node Message Queue. Subscribers may indicate the type of resource and event id on which they wish to receive Predicate Proofs.

Billing and Settlement

Billing is the process of calculating a charge for the use, sale, or transfer of a Resource, or a set of Resources, which can occur in real time, near time, or be period-based. Billing works hand-in-hand with Settlement, which can be real-time, near real-time, or periodic as well.

One of the common uses of Predicate Proofs is the Billing process for a Resource. Resource Owners may;

- control their own fees,
- participate in market based fees, or
- participate in a collective fee setting process.

The Billing process for a resource may be done in:

- **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.

The Predicate Proof must provide the information needed to support the calculation of a charge for the Billing process. All Billing is done on Core Security Nodes, which use a domain specific scripting language for the Billing process.

When Billing and Settlement are both real-time, the Billing and Settlement are atomic with the transaction triggering the Billing on the Smart Meter. This is appropriate for use in zero trust environments. However, real-time Billing with real-time Settlement is the most expensive use of

Network resources, so it also carries the highest transaction cost. In practice, very few real-world transactions dealing with physical goods or services need this type of process.

The calculation of charges is handled via the Billing language, which defines how to calculate a charge based upon the information contained in a Predicate Proof.

The Billing processes may trigger Mining Events, as well as the collection of Revenue. When this occurs, both the revenue and mined assets can be distributed to multiple parties via their Accounting Entity Allocation Tables.

Allocation Tables

Each Resource Owner can set its own allocation tables for Revenue and Mined Asset, or use one of the predefined ones provided by the Network. There are Network-wide allocation tables that all Mining Events and Revenue go through before going to the Resource Owner. For example, the 10 bps Core Security Node fee comes off the top of any value being transferred before going to the Party receiving the value. This is handled by a Network-wide Allocation Table for all value transfers and revenue. Ecosystems and Syndicates (DAOs) may also add an Allocation Table on all revenue for their members.

There are Network wide allocation tables for Mining Events as well. A percentage of all CNDT mined go to the Network Foundation to support further network development and maintenance. A percentage of all mined assets go to the customer and the Core Security Node and Worker Node owners. All of these allocations are governed by Network Governance.

Allocation Tables allow the distribution of revenue or mined assets to multiple parties based on their agreement with each other. These Allocation Tables can be changed at any time by the Party that is the Resource Owner.

Worker Nodes can mine and earn more fees by managing more Resources. Therefore, the number and value of Resources managed by a Worker Node affect the Revenue and frequency of Mining Events on the Worker Node. The value of these Resources also affects the Revenue and frequency of Mining Events on a Worker Node. Therefore, the more Resources and the higher the value of those resources' use, sale, or transfer, the more Mining Events will occur and be more profitable to the Node owners and Network.

Allocation Tables can also be used to allocate a share of the CROP purchased in a transaction processed by a Core Security Node. By default, this allocation is shared between the Core Security Node Operator, the Worker Node Operator, the Resource Owner, the Smart Meter creator, and the Customer. This means that each of these parties can have their own Mining Events occur as a result of the same transaction. This enables Resource Owners to use market economic forces by parties to increase the desirability of hosting their Resource. For example, to increase customer interest in using a specific Resource, or by making it more attractive to run a Worker Node for the Smart Meter that montories a Resource.

Worker Nodes

Each of these Resource owners can use some or all of their fees to buy CROP, therefore they each can mine. The Core Security Nodes treat each of these Resource payments as a separate transaction. Therefore, the fee paid to Core Security Nodes is 10 BPS of what the user pays the app. Core Security Nodes use 100% of their fees to buy CROP so that they mine blocks.

These Worker Nodes can be any device that is used to measure the existence, use, or purchase of something with economic value – a Resource. Therefore, a Worker Node can be any device that can run a Smart Meter that measures:

- The Use of a Resource,
- Recognizes the transfer of the Possession to a Resource, or
- A transfer of Resource Ownership between parties.

Worker Nodes can be communication devices, computers, instruments, IoT devices, routers, or analog sensors that record and measure economic events. For example, communications devices frequently already have the means to measure bytes transmitted, minutes used, bandwidth, sessions, users, etc. Modern operating systems can measure VMs, processes, memory usage, CPU or GPU usage, storage usage, sessions and more. Software running on computers can measure users, duration, access, queries, transactions, etc. IoT devices can measure weight, size, distance, opening, closing and more.

Information about the existence, allocation, capacity, and use of Resources is collected and orchestrated by Core Security Nodes. The entire decentralized Network is controlled economically by these Core Security Nodes. Core Security Nodes manage the Billing for rental, sale and transfer on the Network. A Resource can be the Worker Node itself, content, IP, assets, services or goods that can be measured or monitored via Smart Meters running on a Worker Node, or humans acting as a Worker Node.

Core Security Nodes

All Core Security Nodes must be run on High Trust Node hardware, and cannot run any software other than Core Services on the Node's hardware device. These Core Security Nodes are the most secure and highest trust devices on the Network because they manage all of the Network's Resources and each Parties Secrets. Core Security Nodes are the primary economic actor on the Network because they are Nodes that handle all payment, mining, and transfer of assets or Resources.

However, the Network has two types of transactions; economic and non-economic. Core Security Nodes must handle a significant volume of non-economic transactions, such as authentication, authorization, name resolution, and routing. Non-economic transactions result in no fees or mining. This is why they receive 10 bps on the value of all transactions. They also receive credit for 5% of the CROP purchased by any Worker Node that they monitor. In this way, Core Security Nodes are compensated for non-economic transactions by sharing in the fees and mining activity created by the use, sale, or transfer of Resources on Worker Nodes. All economic transactions have fees, and may result in mining if they include the purchase of some amount CROP.

Parties can use their own private Core Security Nodes to protect all of their secrets and keys, they can share a Core Security Node within a trusted circle, or they can use clustered Core Security Nodes. Even Core Security Nodes in the hands of a hostile party are safe as they have no access to the device. These High Trust Nodes are designed and tested to meet the most sophisticated nation state military requirements for hardware used in situations where the device may fall into a hostile party's hands.

Core Security Nodes provide a common set of Network Core Services. These services protect the Network, enable data to be held in trustless or even hostile environments, route and broker use on the Network's Resources, and handle all Billing and transfer of value on the Network. These services include:

- Accounting, ledgers, key storage, secure storage and wallets
- Data replication, consensus and messaging
- Financial settlement, payments, blockchain bridges and tokenizable assets
- Identity, authentication, authorization and claims management
- Resource management, capacity, location, name resolution and routing

The Core Security Nodes run a DLT based OS that is integrated with a customized version of Linux and can only run on specialized hardware purchased through the Network Infrastructure Ecosystem. This hardware has the highest level of security rating available for hardware devices.

Core Security Nodes are dependent on Worker Nodes and vice versa. Worker Nodes can't mine without Core Security Nodes, and Core Security Nodes can only do a very limited set of mining related transactions without Worker Nodes.

Core Security Node Hardware

Core Security Nodes come in various levels of processing capacity. The processing capacity needed by a Core Security Node is dictated by several factors. The four most important of these factors are the:

- Average number of economic transactions per minute,
- Number of routine trading partners,
- The frequency of access to Resources managed by the Node and
- Size of the desired cache regarding remote Resources.

Core Security Nodes are designed to require as little energy as possible, and to function in highly adverse and diverse environments to be highly-decentralized at the edge. They are designed to maintain security integrity – even if they fall into the hands of a hostile nation state level actor. This requirement dictated the design be entirely built in an entirely sealed unit, which is highly likely to be destroyed if any attempt to access the device's internal components occurs.

The design creates economic trust because the amount of money, knowledge, and time it would take to successfully compromise a unit is uneconomical in a decentralized network where a single computing device holds only a tiny fraction of the Network's data or keys. This necessitates a highly composable design for the processing unit, which is why the Network uses a pluggable, card-based server engineered to increase horizontal processing capacity by simply adding more cards versus large processing capacities per server unit.

High Trust Server Cards

Core Security Node servers are composed of one or more modular High Trust Server Cards as their processing units. These cards are some of the most secure computing devices on the market today. All motherboard components, including the CPU and NVMe SSD, are covered in epoxy and inaccessible. The tamper-resistant High Trust Server Cards are validated for FIPS 140-2 (Level 3), the second highest security rating available from NIST and the highest hardware rating. As such, they are approved for use in high security military and banking environments. Its onboard TPM 2.0 chip, also covered in epoxy, offers additional hardware security through cryptographic key management and a quantum state based random number generator.

High Trust Cards are highly durable as they are coated in protective epoxy, are waterproof, dustproof, fire-resistant and have been tested to run in temperatures ranging from -40°C to 100°C. These nodes have been certified for MIL-STD-810G and are IP67-rated (dustproof and submersible in water for up to 30 minutes). The server hardware has been in use by the US military for multiple years in critical, forward-facing battlefield equipment for use in the US Army's mobile command communications centers, the Apache helicopter, and special forces wearable computers.

High Trust Cards are designed and manufactured in the United States. The Network utilizes a network of certified vendors and maintains a chain of custody of all components, from procurement through shipment. Our supply chain suppliers meet or exceed the requirements for US Department of Defense, and other government agency suppliers of critical infrastructure.

The High Trust Cards are the size of a business card (84mm x 54mm x 6.5mm in size), weigh two ounces and use between 5 or 25 watts of power depending on the model. They are hot-swappable and integrate into all other Network Node Types. Clustered High Trust Cards, and single Quad cards by themselves, can operate at ambient temperatures, but require fan-based cooling. However, Basic cards require no cooling fan.

A Core Security Node (depending on form factor) consists of between 1 to 10 credit card sized hot swappable servers in a single Node. 6 of the 10 card Core Security Nodes can be placed in a 2U rack device. Therefore, up to 6-10 card Core Security Nodes can be housed in a single 2U slot. The Network supports two types of High Trust Cards:

- **Basic** – These cards are appropriate for Core Security Nodes used by individuals, small businesses, and Node Clusters managing less than 100,000 Resources with an average of less than 6 billing transactions per minute per card. These cards require about 5w of power and four can be assembled in a chassis to equal the processing power of one **Quad**.
- **Quad** – These cards are appropriate for Core Security Nodes that deal with a mid-to-large scale business, Registries or Treasuries, high volume transaction environments, or node clusters managing more than 100,000 Resources with more than 6 billing transactions per minute per

card. These cards require up to 25w of power. One of these cards is equal to a cluster of 4 **Basic** cards.

High Trust Node Form Factors

Single-card High Worker Nodes or Core Security Nodes are manufactured in the following forms factors:

- A single card based phone.
- A single card laptop.
- A single card wifi platter addon designed to work in an internal wifi platter tower.
- A single card wifi mesh device designed to work in an external coms mesh network.

Multi-card High Worker Nodes or Core Security Nodes can be manufactured in the following form factors:

- A 1-2 card wifi mesh platter designed to work in an internal wifi platter tower
- A dual card internal tower platter that extends a single basic platter with a Basic card with 1-2 cards either Basic or Quad cards.
- A 2 to 10 card standalone internal use unit.
- An internal 2U rackmount chassis with 2-20 card Core Security Nodes.
- An internal 2U rackmount chassis with 4-60 card Core Security Nodes.

Trusted Time Source

Special versions of the 2U rackmount chassis Core Security Node servers come with a caesium clock used to provide a decentralized High Trust Network Time Source. These time sources are used to develop consensus on an accurate Network Time by all Nodes. These units participate in double allocations from the Service Level mining pool as long as they have maintained a 100% up time within the month.

Accurate Network time is critical for Core Security Nodes which depend on a highly accurate time source for their Temporal Ledgers, as well as Nodes running Proof of Computation for consensus on non-economic transactions. Proof of Computation is a Proof of Work algorithm that requires very little power, but requires special chips to run linear mathematical equations. Temporal Ledgers are unique in the blockchain world because they allow the recording of transactions taking effect in the future to be recorded in the present. This is a unique feature of the Network's Temporal Ledgers.

Core Services Overview

Core Security Nodes run a decentralized set of services referred to as the L0 DLT. However, the L0 DLT is much more than what most people think of when we think about a blockchain L1 platform. That's because the Conduit Network is a hardware and operating system level solution to decentralize the internet, business models and cloud computing. Therefore, the L0 DLT can best be thought of as a new type of trusted internet designed from the ground up based on a new type of hardware and operating system with a DLT of DLTs/blockchains. The job of this system is provide 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** – Resources 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.

For more information on the core services see the Conduit Network Core Service white paper.