# Ontology

A New High-Performance Public Multi-Chain Project &
A Distributed Trust Collaboration Platform

# Table of Contents

Ontology is a blockchain/distributed ledger network which combines a distributed identity system, distributed data exchange, distributed data collaboration, distributed procedure protocols, distributed communities, distributed attestation, and various industry-specific modules. Together this builds the infrastructure for a peer-to-peer trust network which is cross-chain, cross-system, cross-industry, cross-application, and cross-device.

# I TRUST SYSTEMS AND ONTOLOGY NETWORK

## The Three Dimensions of Trust

Trust is a key component in human organization and social collaboration. Trust has become the core requirement of social and economic partnership that has been built up through technology, law, and community throughout history.

### Trust through Technology:

Building trust through technology is seen as a promising area in today's information society. Technologies like cryptology, biological devices, and big data are being used to build trust across industries.

The introduction of blockchain technology has brought trust to the masses through shared access to decentralized information. Blockchain has not just built trust in individual projects - it has fundamentally changed the future of trust ecosystems.

### Trust through Legal Systems:

Trust in legal systems is the oldest and the most basic trust mechanism, assuring rights and protections across industries and across the world.

Economic systems, which are inseparable from legal systems, are a top choice for integration into blockchain. This means a pairing of economic and legal systems is needed to address certain issues including:

> The issue of legal authentication. Due to the decentralized and digitalized nature of blockchains, comprehensive collaboration with offline legal entities is needed.
>
> The issue of legal support. Support for sandbox experiments, automated compliance, and moderation are required for the entire blockchain system.
>
> The issue of identification. Blockchains need to better collaborate with the world to build better identity verification solutions.

### Trust through Communities:

Trusting those close to us can be the most natural form of trust. Sociologists put the number of people we trust at less than one hundred; it is intrinsically difficult to build trust networks on larger scales.

Since the era of informatization and the internet, decentralized network systems such as peer-to-peer networks and blockchains have created online communities much larger than traditional communities. Based on these there have been many attempts to build new communities of trust, such as Google PageRank, Pretty Good Privacy, Web of Trust, as well as other decentralized evaluation systems and decentralized communities.

## Current Issues in Trust Networks

Although we now have a range of trust mechanisms we still face many barriers in establishing trust including:

**Fragmented sources of trust.** When data has to be verified by multiple sources the process can become time consuming, costly, and put data security in jeopardy.

**Missing role of the individual.** Individuals do not have enough say in the use of their own data and authentication of other data.

**Emergence of new sources of trust.** With fragmented sources of trust the overall cost of verification has increased.

**Data management monopolization.** Today's data management systems are monopolizing user data while failing to compile useful and accessible portfolios of data for external use.

**Data fragmentation.** Due to fragmentation of databases, data which is not monopolized loses out on trading potential and can often not be authenticated and used.

**Inaccurate identity verification.** Using a single information management system makes it difficult to form comprehensive identity portfolios.

**Security issues in the Internet of Things.** Currently there are not sufficient identity verification mechanisms to prevent illegal and malicious node access to the Internet of Things.

**Data exchange security issues.** Current data exchange systems are centralized, which causes problems such as loss of data origin and threats to data security.

**Trust issues in collaborative systems.** Without a central authority it is difficult to form trust in collaborative systems.

**Transparency issues in equity management.** New equity management models such as crowdfunding find it hard to build trust due to lack of transparency.

**Weak community management.** Current community management systems do not have sufficient moderation tools.

**Identifying false information.** There are not sufficient mechanisms to identify, report, and remove false information from online systems.

**Weak reputation systems.** Adequate reputation systems require massive data sets, however fragmentation of data in current systems does not make this possible.

**Making charitable donations.** It is becoming more important to provide high levels of transparency when managing charity donations. Basic transaction tracking can only solve part of the problem; comprehensive verification of organizations and recipients is needed.

The variety of trust mechanisms at hand today have indirectly become the weakness of today's trust systems. Building a network which integrates the fragmented industry is needed to build a true and complete trust system.

## Ontology's Ethos

Ontology has architected a distributed trust system. It incorporates multiple trust types in an integrated protocol system with various blockchains and databases. Multi-source identities and multi-source data exchange protocols have been implemented into the network, building a distributed trust system that is cross-chain, cross-industry, cross-system, cross-application, and cross-device.

Ontology aims to develop its trust ecosystem through partnerships to provide distributed services including distributed communities, data verification, data exchange, and credit across industries.

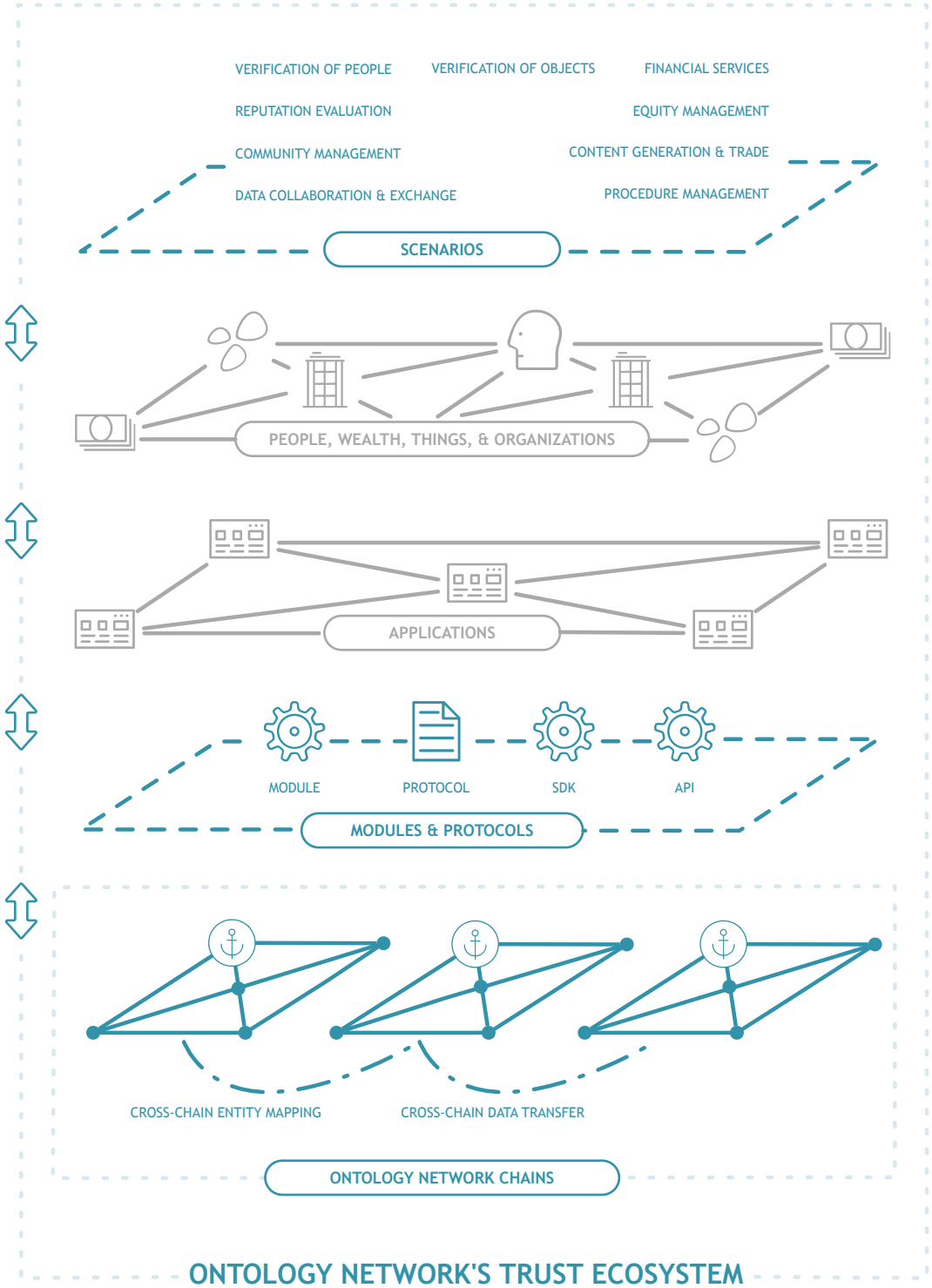
## Vision and Structure

Ontology's Trust Network is a protocol network built with multiple blockchains and systems to support use with all business types.

In order to meet the needs of different industries, the flexible design structure is modularized, pluggable, and easily expandable.

Ontology applies blockchain technology to all business types, providing blockchains, smart contracts, distributed verification management, data exchange, and other protocols and APIs. Users can easily develop distributed services through Ontology without having previous knowledge of distributed networks.

> An integrated and diverse distributed trust network and the tool for building a trust ecosystem



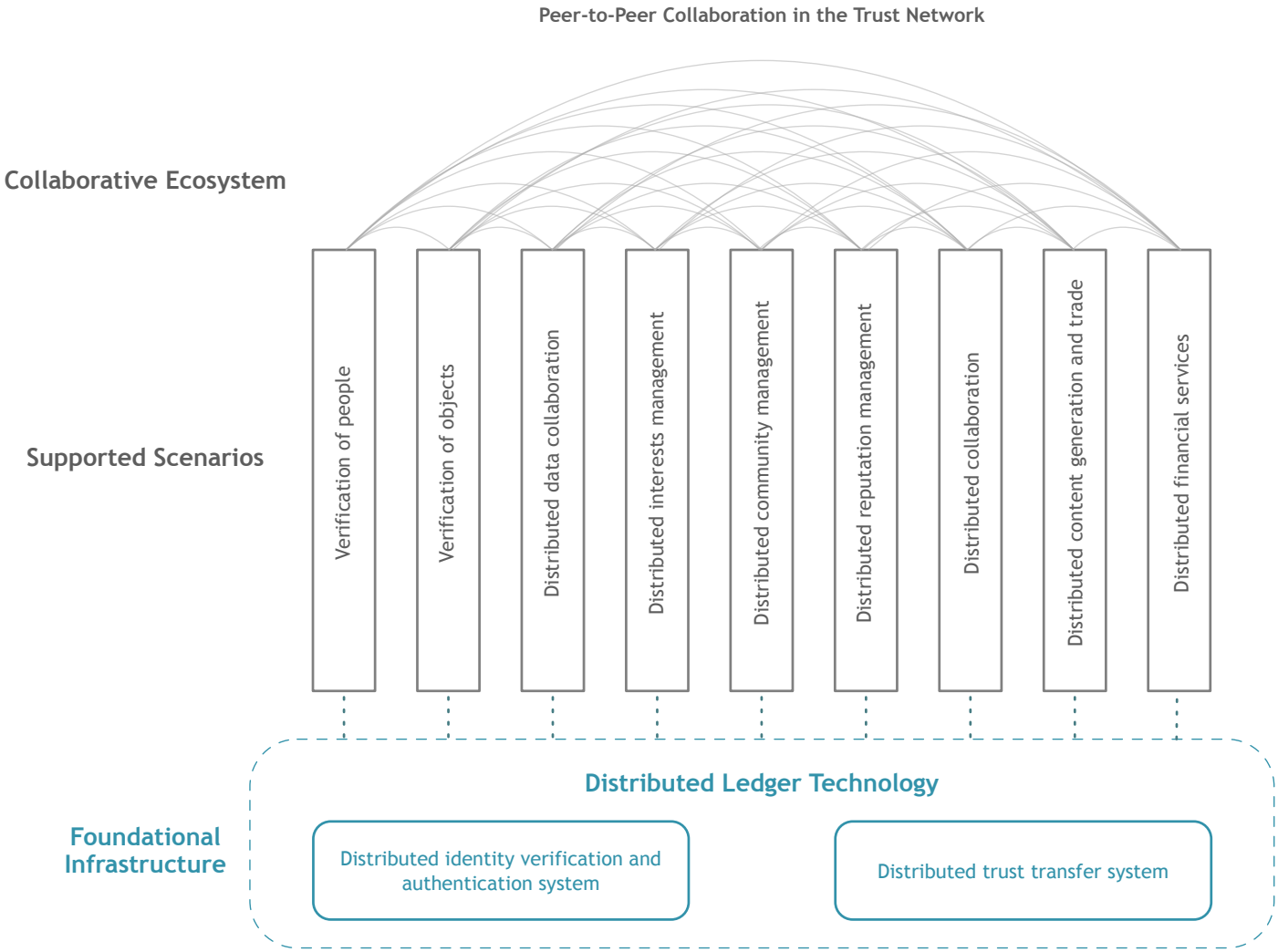

ONTOLOGY NETWORK'S TRUST ECOSYSTEM

# II ONTOLOGY TRUST NETWORK

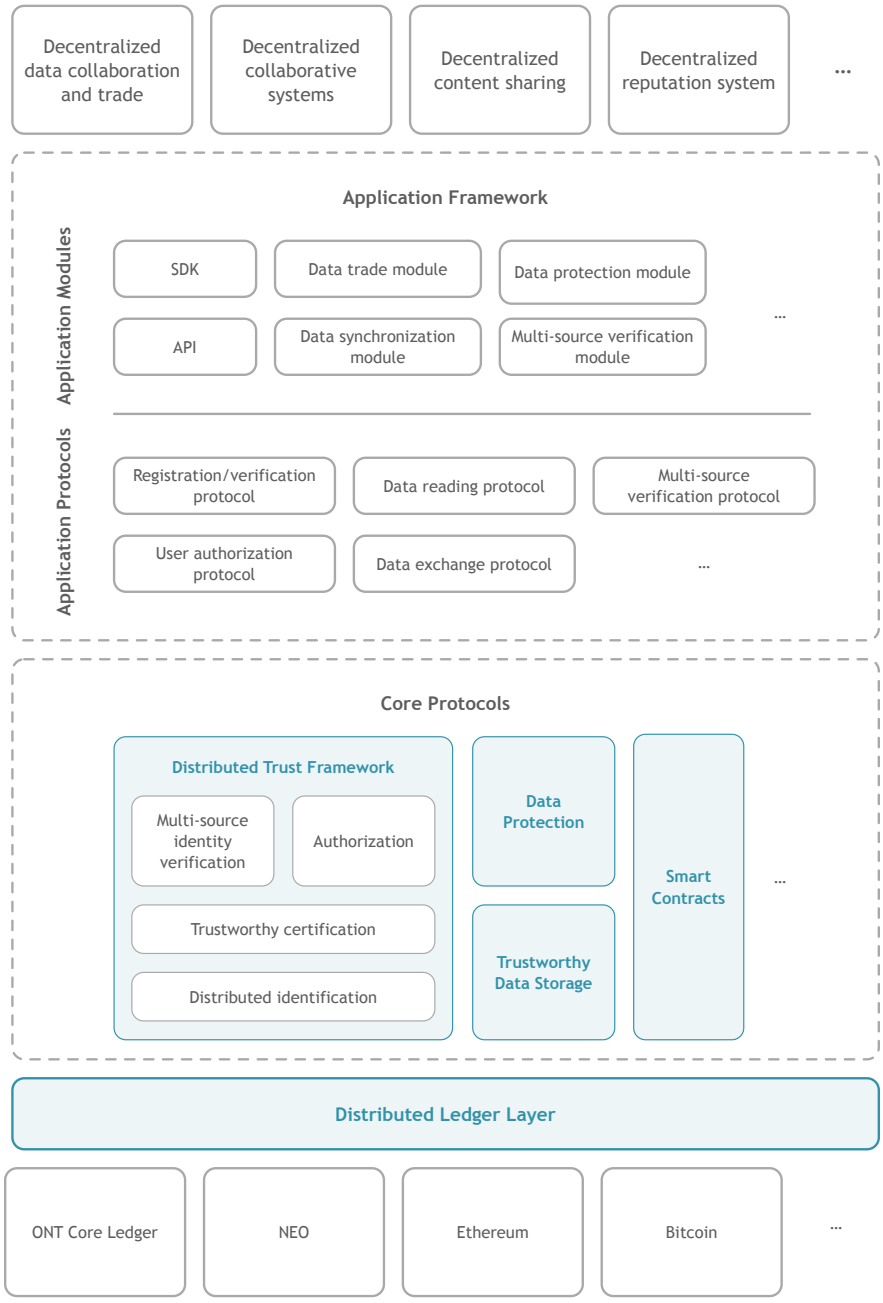
## Ontology's Trust Ecosystem

Ontology is devoted to building a trust ecosystem through its decentralized services.

With Ontology's infrastructure industries can integrate and develop their own systems of trust.


Peer-to-Peer Collaboration in the Trust Network
Collaborative Ecosystem
Supported Scenarios
Verification of people
Verification of objects
Distributed data collaboration
Distributed interests management
Distributed community management
Distributed reputation management
Distributed collaboration
Distributed content generation and trade
Distributed financial services
Distributed Ledger Technology
Foundational Infrastructure
Distributed identity verification and authentication system
Distributed trust transfer system

## Ontology's Framework Technology




At Ontology's foundation is a fully decentralized ledger system that includes smart contracts and security protocols. Ontology provides compatibility support for complex technological systems, whether that be existing blockchains or tradition information systems. All systems feature decentralized entity management with support for main protocols and different password standards.

Ontology also provides systems for secure data storage, hardware options for key management, and encrypted data analysis. Together this creates an application platform that allows for all kinds of services to become decentralized.

Ontology provides the framework for use of all type of applications, including decentralized data exchange and procedure management protocols through the use of APIs, SDKs, and other modules.

## Decentralized Identity Verification and Multi-Factor Authentication

A decentralized and multi-factor identity verification system that assures data privacy is core to building a trust network. Such a system can provide identity verification systems for individuals, organizations, and physical objects.

### Multi-Factor Authentication

Ontology's identity verification system is characteristically decentralized. Decentralized identity verification is not predefined by industry nor does it come with set features, it is instead built by project-specific requirements.

### Organizational Identity

Organizational networks can be established using information such as student IDs for academic institutions or employee IDs for businesses. All entities can select a range of identity verification methods in order to create systems free from third party interference. Private information is securely stored in decentralized databases.

### Specialized Identity Verification

Entities can create specialized identity verification systems based on industry-specific or legal requirements, for example by integrating compatibility with external electronic identification system such as CA Identity Manager, or by integrating requirements of governments, organizations, academia, businesses, or social groups.

## Delivering a Decentralized Trust System

In Ontology a decentralized trust system can be implemented alongside traditional trust systems. This includes:

### Community Trust

Community trust is an effective system in which communities and individuals play an active role in identity verification.

### Trust Anchor

A trust anchor is an entity that has been entrusted to conduct identity verification. The higher the trust in the trust anchor, the higher the trust in the network.

### Statement

A statement is the medium of community trust. In Ontology a statement is a confirmation passed from one entity to another; only one statement is needed to instantly verify information.

### Trust Transfer

Trust transfer is conducted by submitting information required and receiving a statement. This could be an individual submitting their own identity information or using previously submitted information to form a portfolio of multiple identity certifications.

## Distributed Ledger Technology

> Ontology's storage system works on a distributed ledger. The key feature of the completely decentralized, tamper-proof ledger is that trust is shared amongst multiple parties through the use of smart contracts, distributed networks, distributed storage, distributed authority, distributed security, and a variety of modules.

### Entity Registration and Authorization

An identity registration and authorization system can be built with Ontology's adjustable configurations or by using a third-party authentication system such as CA Identity Manager. Community authentication and industry-specific verification methods can also be used to allow participants access to identity verification through the blockchain.

### Data Directory

Data can be registered categorically to directories and use data identifiers (ONT Data ID) and data resource identifiers (Data URI) to match and verify to requirements through the decentralized system.

### Procedure Protocols

Ontology's procedure protocols are carried out with distributed ledger technology, cross-chain entities, cross-system privacy, and cross-chain protocols.

### Data Exchange

All entities using Ontology can use the data exchange. It allows users to have full control of their data; having the tools to trade it while being able to meet their own privacy requirements.

### Data Attestation

The distributed ledger system does not only store data but also records its use. Each data request, data matching, data transfer, and data usage is attested to the ledger, forming a complete private record of the data use.

### Smart Contracts

Businesses can grow by implementing smart contracts and trust networks through new procedure protocols, controls, and exchanges of data.

## Distributed Data Exchange

Ontology supports distributed data exchange, which includes:

### Peer-to-Peer Data Transmission

The data exchange system uses blockchain to support accurate search and transmission of data between two parties without having a centralized database.

### Data Authorization Mechanisms

Data privacy protection and leakage prevention are always assured whilst giving the user full control of their data; each data transfer must receive authorization from all parties.

### Copyright Protection of Data

Ontology stores, manages, and attests data throughout its life cycle. A digital identity is created for each copy of data from registration, request, authorization, to exchange. Copyright protection is also recorded to each copy on the blockchain.

### Distributed Data Storage

A distributed data storage layer supports decentralized storage for different types of data.

## Other Key Functions and Modules

### Ontology Crypto Package (OCP)

Ontology provides a series of cryptography and data security module support in areas including multi-factor entity authentication, distributed data exchange, and distributed procedure protocols. This includes encrypted data transfer, key sharing protocols, multi-party key management, ring signature modules, blind signature modules, and secret sharing mechanisms. In identity and data validation zero-knowledge proof and homomorphic encryption schemes are used, and in a collaborative application two records are kept. Other multi-party technology schemes are being explored for the future.

### Ontology Marketplace (OM)

Ontology Marketplace is a distributed data exchange complete with data sets, algorithms, and models. It acts as an extension to Ontology, providing data products, data predictions, and data computing resources. At the same time it maintains compatibility with other major cross-chain systems to create a large data exchange platform. The native dApp lets providers across industries implement the data trading market.

### GlobalDB

GlobalDB is a distributed key-value storage. It provides multiple backend database module options including levelDB, RocksDB, TiDB, and cockroachDB.

GlobalDB is a blockchain database and IPFS module. GlobalDB provides the ability for distributed transactions, scalability, real time checking of the blockchain, and ability to interact with data off-chain. It can be used to correlate the blockchain and data, the blockchain and AI, and so on.

Ontology will build further modules according to project-specific requirements.

### HydraDAO

HydraDAO is a data prediction and interaction module integrating smart contracts, cross-chain, and cross-data source collaboration. It contains Ontology's DAO (distributed autonomous organization) and cross-chain data interaction (big data/AI) features. Ontology's governance mechanism supports democratic and AI-automated propositions and verifications. A unique DAO address and polling token will be created during the process, which allows DAO to automatically add funds and results to Ontology. Once polling is complete, DAO will autonomously execute in accordance with the tamper-proof smart contract. The mechanism allows data exchange and governance in Ontology to function with flexibility and supports the technology for large-scale automated network operations.

### Ortorand Consensus Engine

Certain distributed ledger networks within Ontology's chain network support Ontorand Consensus Engine (OCE), a new consensus engine. Ontorand is a highly effective version of the DBFT consensus protocol based on Onchain's Distributed Networks Architecture (DNA). It has reached near-infinite scalability and requires a relatively low hashing rate, making it highly unlikely to experience forks of the network. Ontorand's block-creation speed is only limited to internet speed, usually resulting in confirmations within 20 seconds. As a truly decentralized protocol, Ontorand entitles its users to consensus rights, eliminating cases where miners or other parties solely control confirmation power. Ontorand selects who confirms the blockchain using a verifiable random function, every confirmation receiving an Ontology seed directing to the next confirmation. Ontorand also supports pluggable verifiers and online protocol recovery and upgrade. Meanwhile, in order to meet needs from different chains in Ontology, the distributed ledger framework also supports pluggable consensus mechanisms including DBFT, RBFT, and custom PoW.

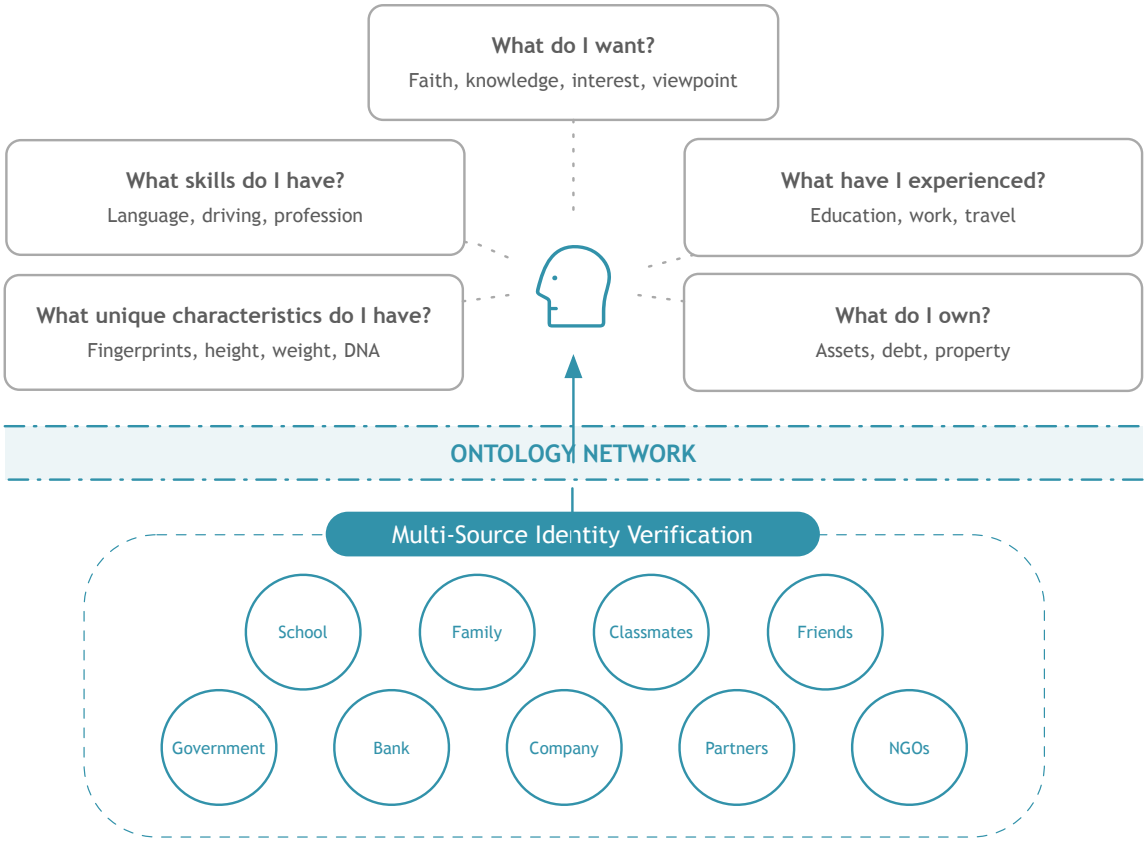
# III ONTOLOGY'S ECOSYSTEM AND APPLICABLE SCENARIOS

Ontology helps its partners improve their systems by integrating them into the blockchain infrastructure and designing comprehensive applications that come with full technical support.

This part will introduce some of the applications that can be built onto the network.

## Multi-Source Identity System for People

> Users can collect and manage their own identity data from various sources including public institutions, banks, businesses, family, colleagues, and friends.




### Multi-Source Identity Authentication

Multi-source identity authentication is the verification process of an identity by more than one source to give it a more secure and trustworthy certification.

### Comprehensive Personal Profile

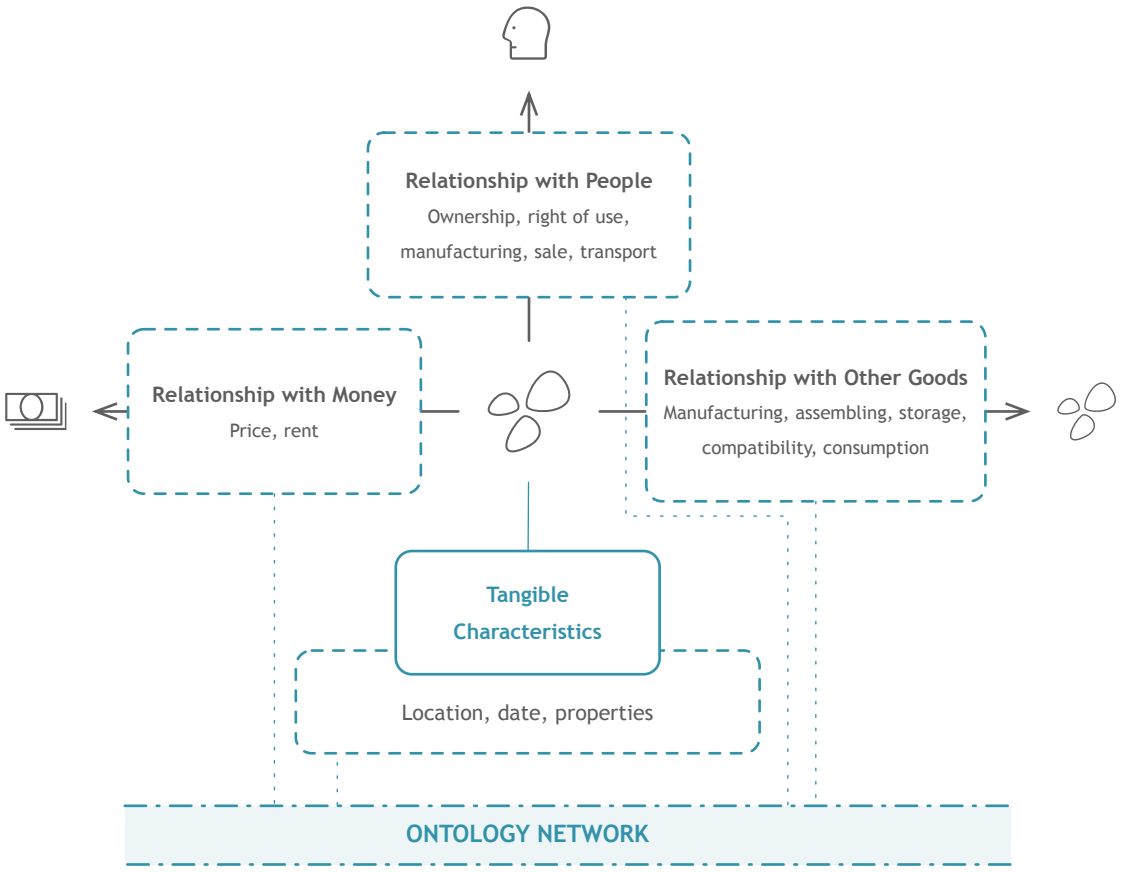
A comprehensive personal profile describes the state in which an individual has built up an identity with data from multiple sources relevant to them.

### Data Tracking

All authentications on Ontology are performed with signatures, which cannot be forged or repudiated. Meanwhile, to assure a secure authentication system, authenticators themselves can be subject to review if their authority or trustworthiness is questioned.

## Multi-Source Identity System for Objects

> In Ontology you can register digital identities of physical objects into the distributed network under the supervision of the product owners and/or producers. Each object has its own API and can interact with other digital identity holders.




### Object Authentication Cycle

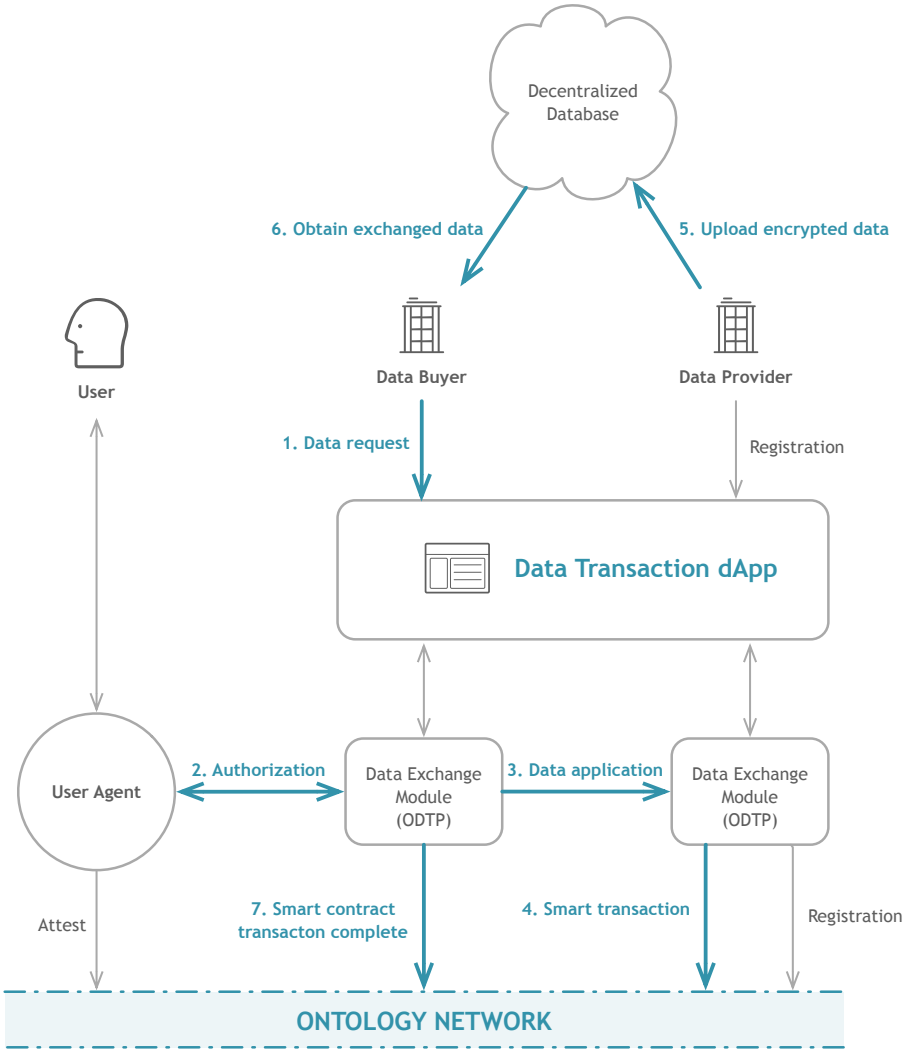
Objects can be tracked throughout their life cycle with multi-factor authentication by:

- Registering digital DIDs onto Ontology.
- Verifying objects with digital signatures and endorsement verification.
- Tracking the use and any other related data.

### Object Data Recording and Authentication

Ontology can fully record and authenticate object data including ownership, circulation, user behavior, and other relevant information.

## Distributed Data Exchange




### Data Discovery

Data on a single entity no longer has to be manually gathered from multiple sources. In Ontology a comprehensive portfolio of data is already compiled and can be accessed with the user ID, allowing for easy data collection and use.

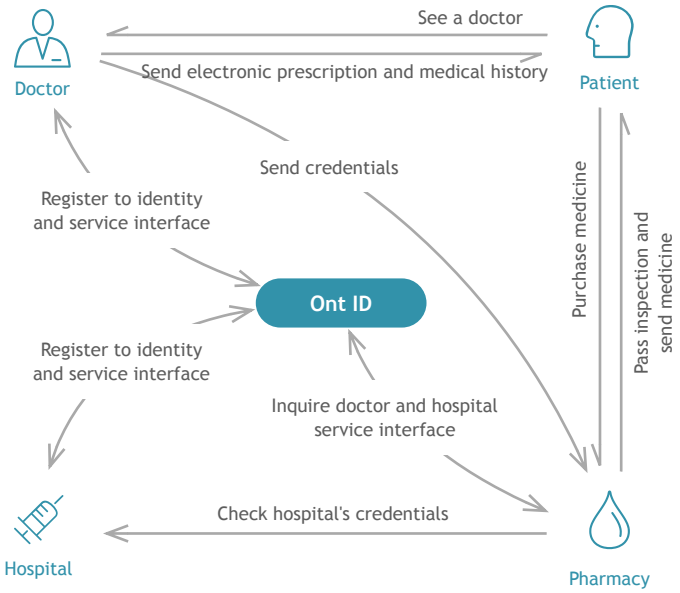
### Data Exchange

The data owner must accept the data request before the data is exchanged and the users credited.

User online behavior data is often stored by service providers for analysis and trade. Ontology provides a data exchange system in which all data (with consent of the owner) can be discovered and traded to the owner's benefit whilst meeting individual privacy requirements. By nature of blockchain and smart contracts, all records on Ontology are open, transparent, trackable, and tamper-proof. This technology can be applied to areas including signing certificates, joint credit, distributed collaborative computing, and AI training data.

## Distributed Collaborative Systems

Distributed collaborative systems in Ontology help build up the trust network.




### An example of distributed collaborative systems in medicine:

When doctors, hospitals, and patients register their identities onto the blockchain, the blockchain fills in the trust gap between the pharmacy and patient with record of the medicine's key information. The pharmaceutical enterprise then sells the prescribed medicine to the patient after verification of the doctor and hospital's credentials.

### Authorization Records

Modifiable authorities of each participant are recorded and confirmed by all relevant parties.

### Activity Records

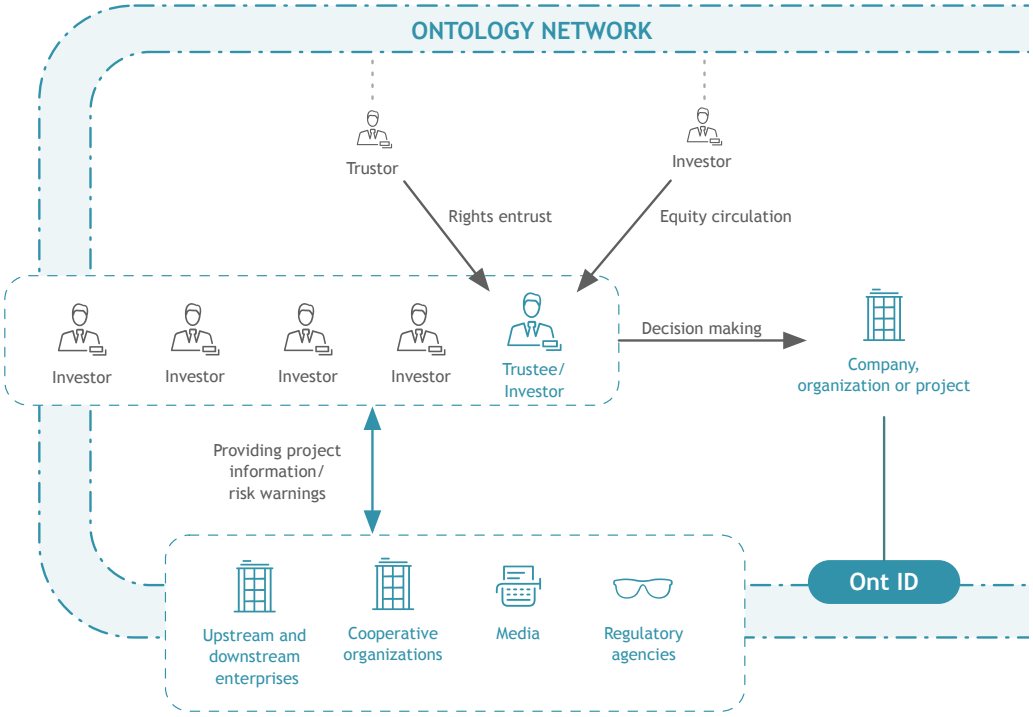
All activity is recorded to ensure transparency of participant identity, activity, and outcomes.

### Evaluation

A multi-party confirmation and endorsement mechanism allows for evaluation of collaborative entities.

## Distributed Equity Management

> Today's economic system contains a range of equity management models, though due to factors such as low transparency and information asymmetry these projects lack credible trust mechanisms. Equity management is also facing obstacles regarding project assessment, risk warnings, information disclosure, equity circulation, and authority entrustment. In light of this Ontology has built a trustworthy distributed equity management system.




### Example in Investment Management:

Ontology has the functions to:

Safely circulate data by having the option to include factors such as basic project information, operation status, risk warnings, and records.

Create a multi-party assessment system to include project operators, investors, cooperative organizations, and upstream and downstream enterprises in which parties provide information on each other.

Manage a project evaluation system where data can be accessed and assessed by its investors.

### Distributed Interests Configuration

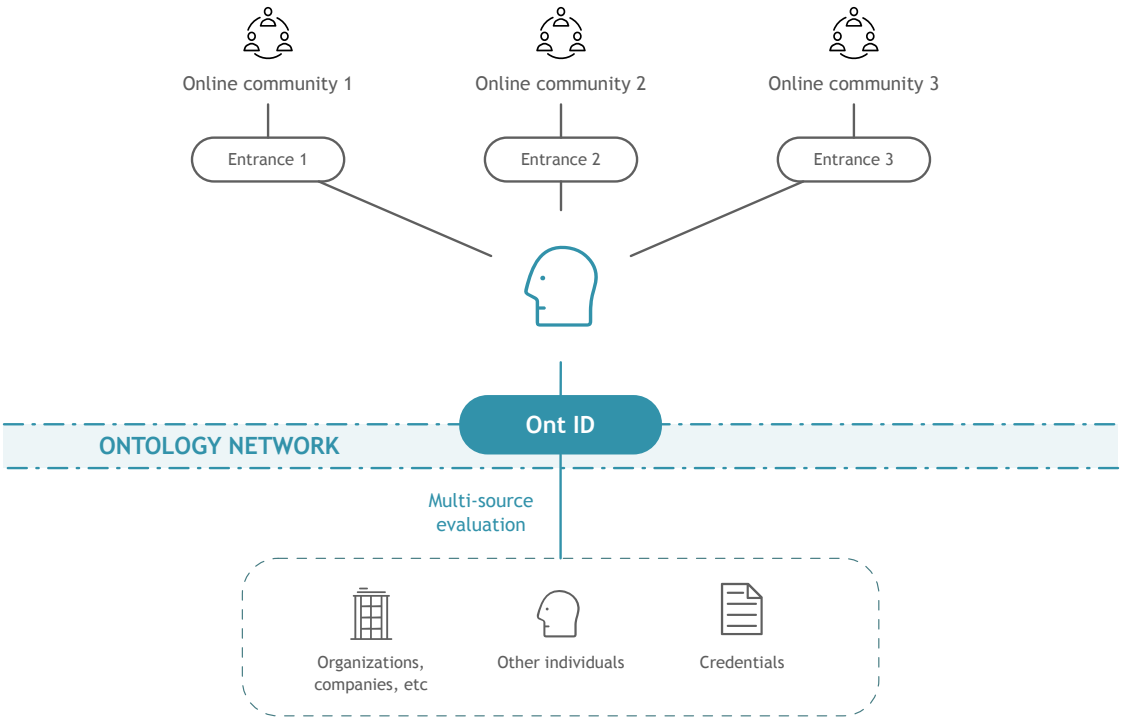
Interests configurations are transparent to all parties and recorded onto the blockchain.

### Distributed Rights Entrustment

Ontology allows for multi-party rights entrustment and recording, including the function to dispute actions by providing relevant data.

## Distributed Community Management

> Current online communities are run by centralized service providers. Ontology provides the framework for communities to run in a purely decentralized system.




### New Member Control

In Ontology community managers can build their communities steadily by managing the inflow of members into the community.

### Community Ranking

Most communities have ranking system where different users hold different levels of authority and discourse power. In Ontology users can present their DIDs or other evidence of experience (for example someone presenting proof of a Java community group they manage) to community managers to receive recognition.

### Other Features

To address the difficulty of certifying an individual's authority and credibility within a distributed community Ontology has integrated:

A public credibility system. According to the personal details, publication history, and chat history of an individual, the community can carry out multi-party evaluation of community members to reward public credibility.

Content publication control. Controlling false or inappropriate information in distributed communities is essential. Ontology offers a system where users with authority can directly push content and ordinary users must first pass content approval.

An incentivization design. A reward mechanism recognizes content creators for the reactions their content receives from other community members (such as “likes”). All content reactions are recorded to the blockchain to avoid data manipulation.

## Distributed Content Generation and Trade Modules

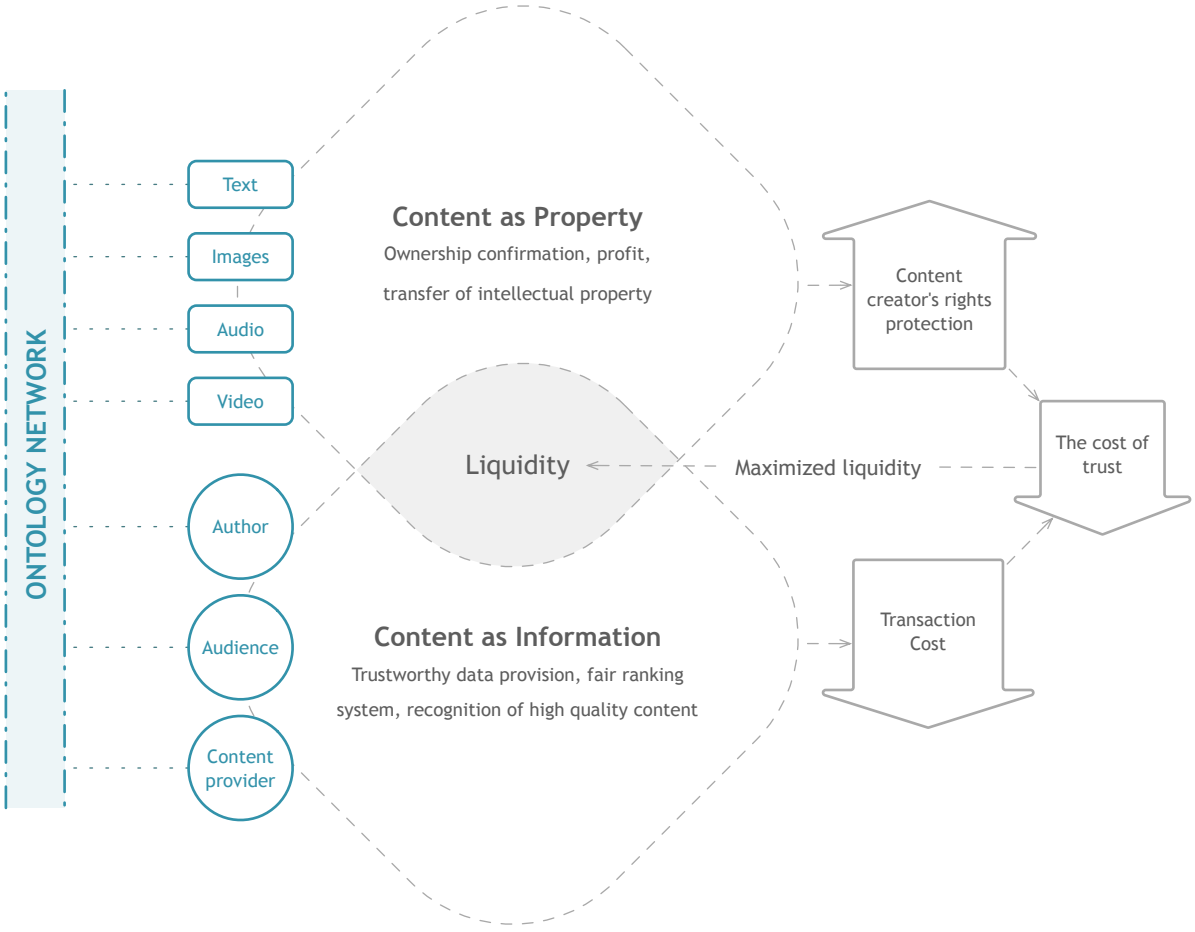
Current services can convert content into tangible assets (e.g. paid content) or into other types of intangible assets (e.g. content publishing with a profit model), though nevertheless at a cost to the content producer. Ontology, however, has introduced a comprehensive distributed trade system between content generator and consumer.

### Optimized Content Search

Users can choose to only view content produced by users with a certain reputation level or entrust third-parties for content recommendations. In this system users have greater control in getting the content they want and can getting a fairer price for it.

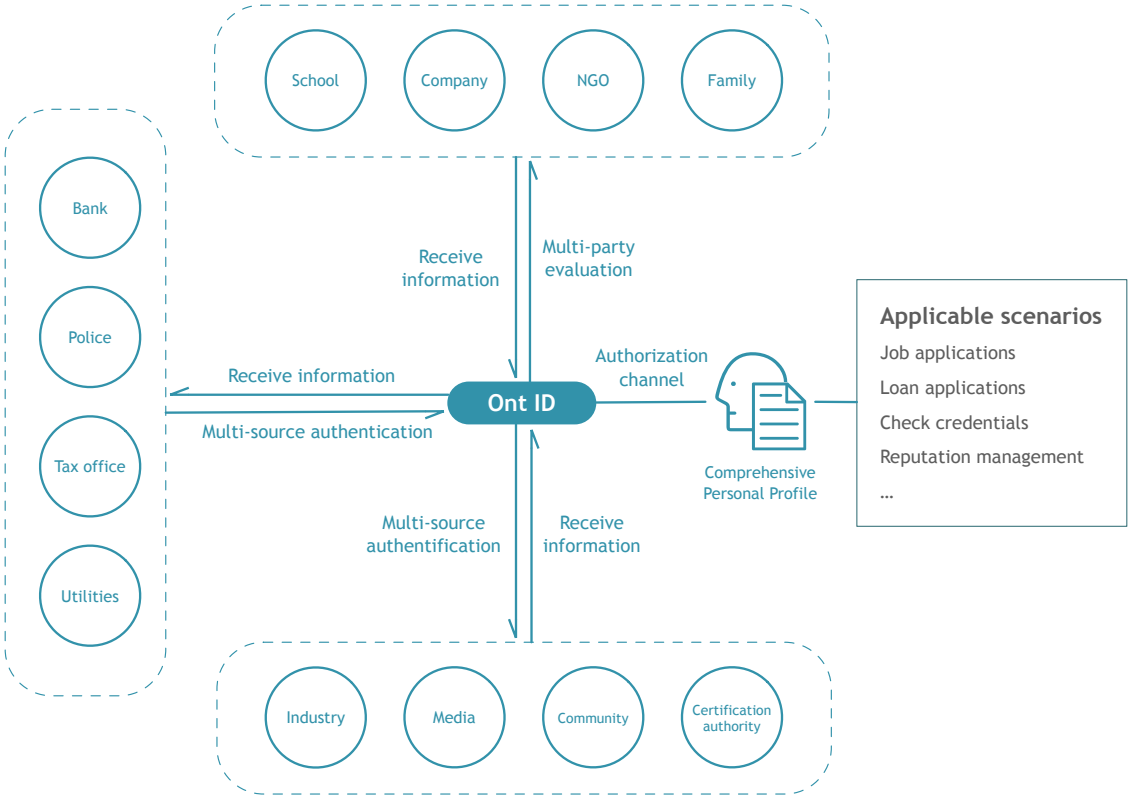
### Content Security Guarantee

Ontology's tamper-proof identification system can function with legal validity. Since blockchain is an open source third-party technology, users can carry out IP legal right authentication, payments, and transfers worldwide. The reputation system helps build a reputation-based protection for content that adds another layer of security to the content exchange system.



## Distributed Reputation System

In our daily lives we have to provide valid proof of certification for personal endorsement, for example with academic certificates. A reputation on the other hand is seen as a weak form of validation.




### Credit Management

Ontology calculates local and global trust levels according to modifiable criteria. Local trust calculation uses local evaluation parameters and opinions, whereas comprehensive trust uses global evaluation parameters to assure certainty and diminish the influence of false information.

### Data Management

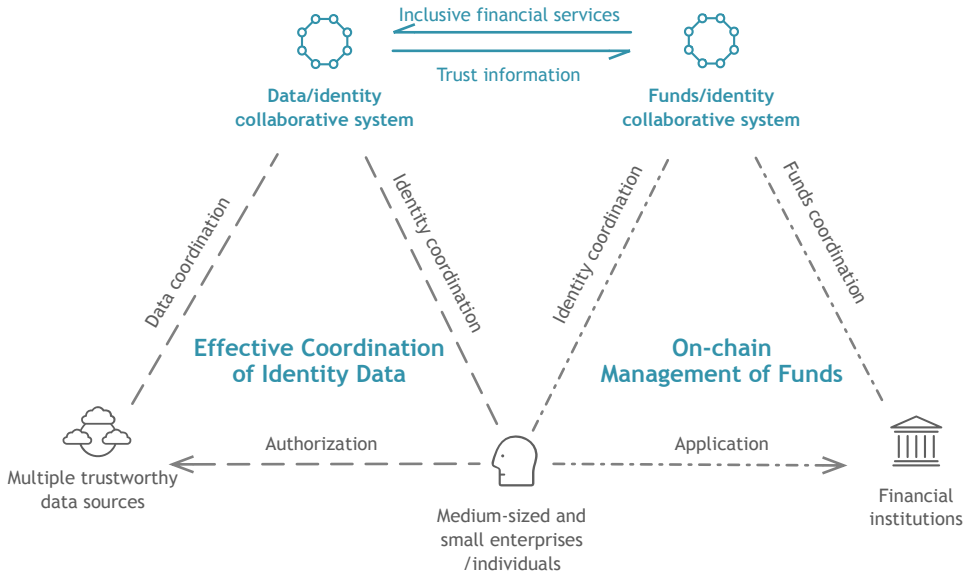
Ontology combines two types of trust data management models: one storing data in a completely decentralized system and another storing data partly in centralized management systems where needed.

### Building on Trust Models

Trust models can be further developed by collaborating with the content generation and exchange system, for example by using multi-source or multi-factor authentication systems for content evaluation and verification.

## Decentralized Inclusive Financial Services

Small businesses and individuals often lack credit records and collateral while facing high operation costs. This makes them riskier for banks and other financial institutions, leading to high interest rates. At the same time the cost of change is high and businesses face retributions to their reputation if they do not comply, leading to a multifaceted dilemma.




### From a Financial Aspect

Ontology helps businesses and Ontology helps businesses and individuals become active managers of their data. With multi-source data coordination and authorization individuals can easily and safely provide information to apply for financial services and receive fairer interest rates from reducing risks to the other party.

### From a Social Aspect

Financial institutions can also collaborate with Ontology, establishing multi-party security coordination and analysis mechanisms to provide better interest rates and services to small businesses and individuals.

## Applicable Scenarios

Ontology can provide distributed infrastructure to a range of scenarios without service providers having previous knowledge of distributed networks, blockchain, or cryptography.

Listed below are scenarios that can benefit from integration into Ontology:

**Finance**

- Trading
- Securities
- Wealth management
- Derivatives trading
- Collateral management
- Supply chain finance

**Payments**

- Micropayments
- Business-to-business international remittance
- Tax filing and collection
- Know your customer (KYC)
- Anti-money laundering (AML)

**Insurance**

- Claim filings
- Claims processing and admin
- Fraud detection
- Telematics and ratings
- Digital authentication

**Internet of Things**

- Device-to-device payments
- Automated operations
- Grid management
- Smart home management
- Office management

**Consumer**

- Sharing economy
- Supply chain
- Pharmaceutical tracking
- Agricultural food authentication
- Shipping and logistics management

**Media**

- Digital rights management
- Art authentication
- Ad placement
- Ad click fraud reduction
- Resale of authentic assets

### Software Development

- Micritization of work
- Disbursement of work
- Ad placement direct to developer payments
- Ad placement API platform
- Ad placement notarization and certification

### Medical

- Record sharing
- Prescription sharing
- Multi-factor authentication
- Personalized medicine
- DNA sequencing

### Asset Titles

- Diamonds
- Designer brands
- Car leasing and sales
- Home mortgages
- Land title ownership
- Digitalization of assets

### Government

- Voting
- Vehicle registration
- Benefits distribution
- Copyrights
- Education certificates

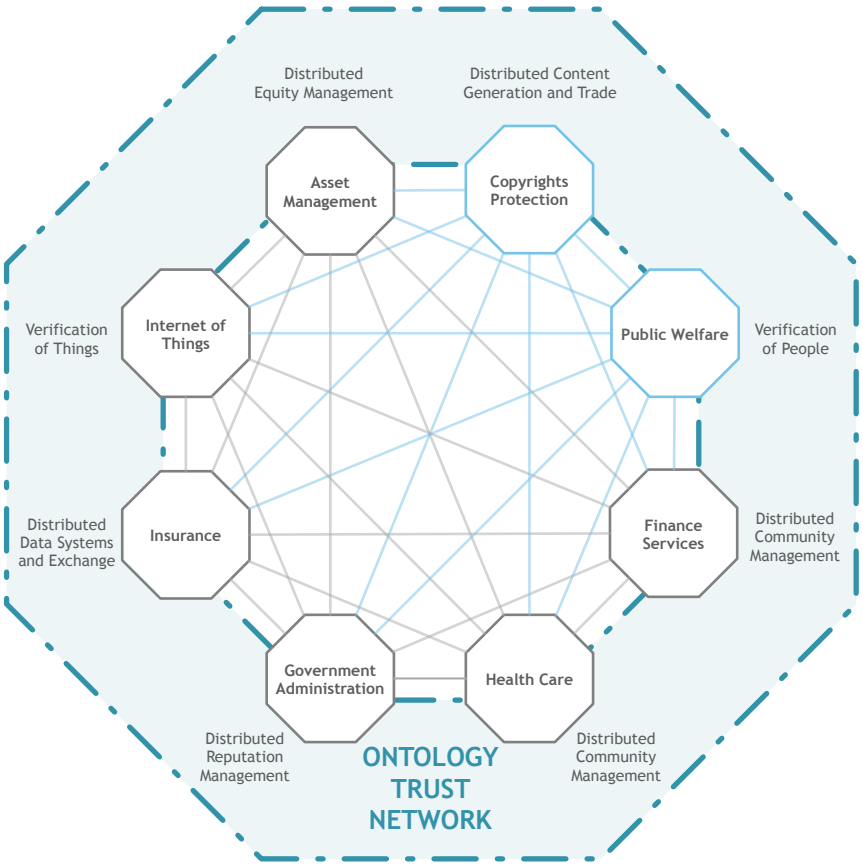
# IV

# ECOSYSTEM / GOVERNANCE/ INCENTIVIZATION

## The Ontology Family

Ontology is built to be the **foundational infrastructure of a trust ecosystem**, supporting the development and upkeep of decentralized technology and data systems while acting as the connector between networks so that partners only need to focus on their business operations.

Ontology Family are the major partners in the Ontology ecosystem. The following are the groups that make up the Ontology Family:




### Verification Service Providers

Electonic identification, CA Identity Manager, and other publicly credible identity verification service providers for institutions, companies, organizations, social groups, and individuals.

### Application Service Providers

Cross-industry application teams establishing their own projects on top of the Ontology infrastructure are core to the Ontology Family. At the same time Ontology helps services succeed at their projects by helping with the creation and development of applications.

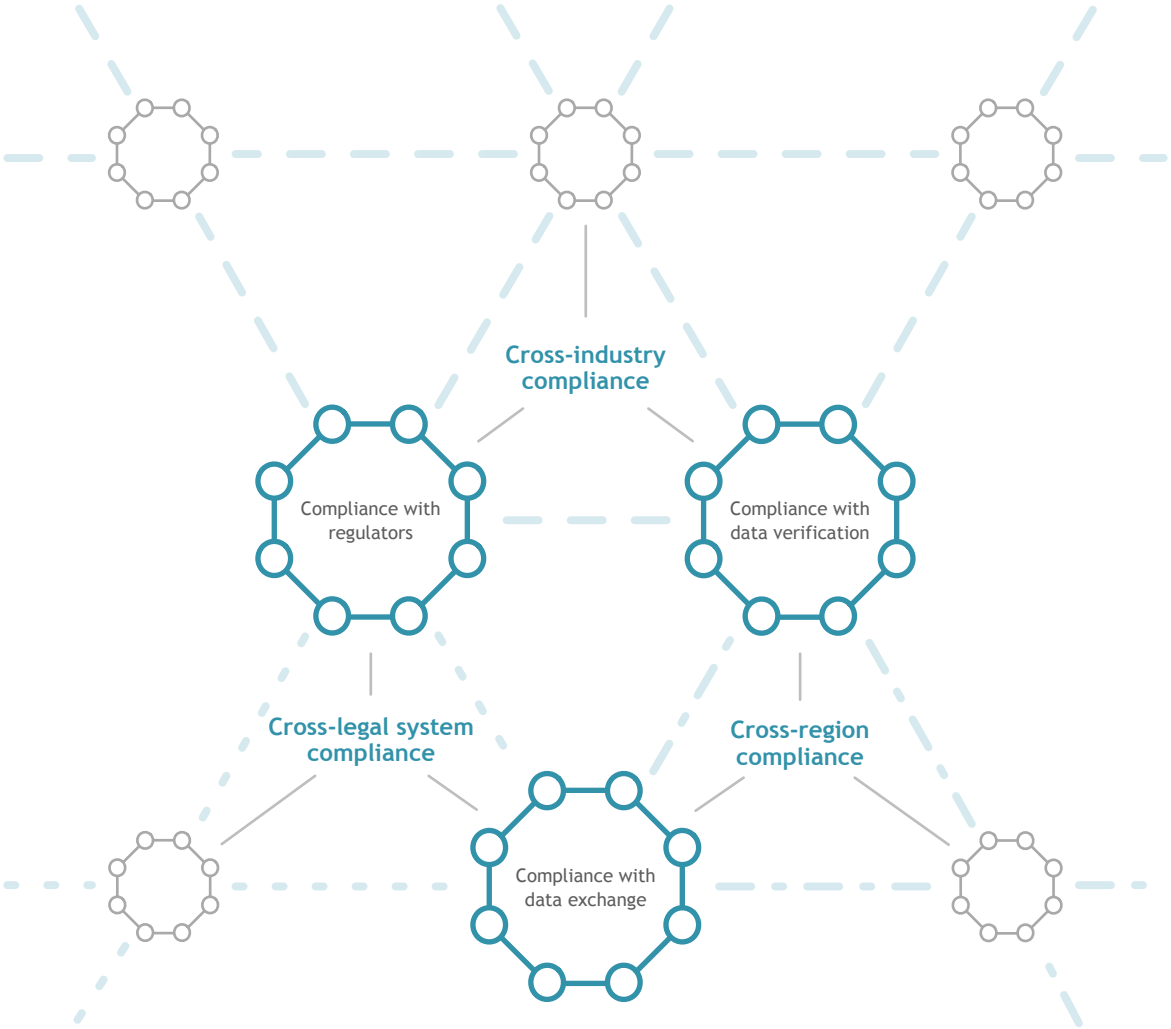
### Communities

Communities in Ontology can pool together global institutional and individual-level talent to create an ideal environment for sharing and growth.

### Individuals

Individuals act as fuel to the Ontology ecosystem, powering the authentication and endorsement systems whilst helping expand the decentralized communities.

## Compliance




**Ontology Network's Compliance Support**

Cross-industry cross-chain compliance

Cross-legal system cross-chain compliance

Cross-region cross-chain compliance

Ontology's identity verification and data systems are compliant with the various legal frameworks in different regions and industries across the world. To accomplish this Ontology has built in mechanisms to easily integrate legal framework into the ecosystem, making it easy for all entities to be compliant across the board while securing Ontology's status as a secure decentralized trust network.

www.

ont.io

## Contact Us


Email: contact@ont.io

Telegram: OntologyNetwork

Twitter: OntologyNetwork

Facebook: ONTnetwork