ONTology

Ontology Trust

Framework White Paper

Version 2.0.0

2019/07

Abstract

Through history, people have established trust from different dimensions and methods, for instances, via technology, legal system and communities etc. However, multi-source, multi-system and multi-method single-point trust collaboration will incur very high collaboration costs, hindering the depth and breadth of trust collaboration. Although internet technology changes rapidly, but the pain points of trust still exist today, such as trusted source decentralization, data fragmentation, lack of individual roles, identity verification and difficulty in identifying false information. During the collaboration process of society governance, economic collaboration, and financial service, there is a large amount of cost incurred by "trust" every day.

The decentralized and tamper-proof blockchain has built technology trust for specific scenarios from a certain mechanism. However, to integrate with more business scenarios in real world requires more integration mechanisms. How to construct a trust mechanism that combines diversified trust and integrative applications becomes the pursuit for the new "trust" infrastructure.

Ontology is committed to building a systematic, streamlined, and integrated trust ecosystem. Ontology will serve as the infrastructure and connector for trust ecosystem, providing a complete blockchain infrastructure for the effective collaboration of trust sources, the interconnection of data sources, and the distribution of various types of distributed application services.[1]

1. Ontology is an infrastructure that supports multiple trust collaboration scenarios and will continue to extend various modules and protocols based on scenarios and application scopes of applications. This Trust Framework White Paper only describes Ontology's planning at the current stage and will be continuously updated according to the actual project process.

This White Paper focuses on the Ontology trust framework.

Table of Contents

1. Introduction

This White Paper describes the Ontology trust framework, including the service layer tool, the platform layer application module and the Ontology application protocol.

- Ontology service layer: Based on the Ontology core layer, Ontology provides modular service layer tools to improve the scalability and flexibility of the infrastructure on the whole.
- Ontology application layer: It provides an upper layer application platform based on identity and data asset, providing a solution for information assetization and asset transaction, to build Ontology's public service platform. It also supports cross-chain call. The application layer also supports cross-chain solution for heterogeneous chains.

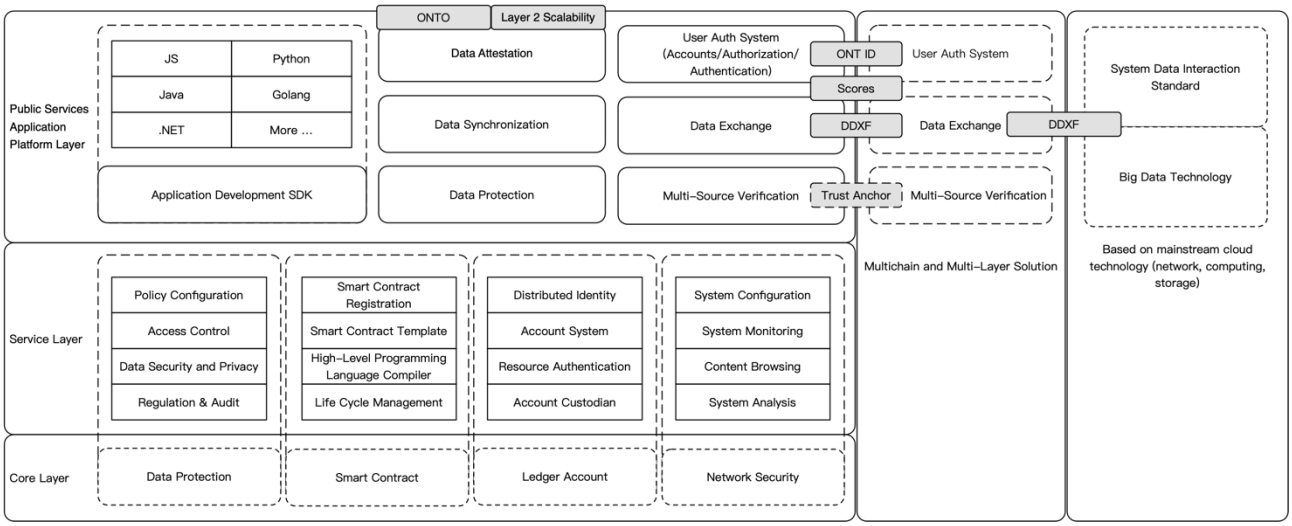

Figure: Ontology Trust Technology Architecture

Ontology uses its trust framework to build the Ontology trust ecosystem: the Ontology blockchain infrastructure provides tamper-

proof and data security services; the Ontology data exchange framework offers trusted data service, including data processing, privacy protection and secure data storage; the Ontology identification protocol provides a consistent identity verification and Auth services for data ownership authentication and data processing.

The Ontology trust framework is the core logic layer for Ontology to achieve distributed trust. It connects people, assets, things, and affairs with the decentralized identifier ONT ID, which is decentralized, self-sovereign, easy to use with data protection and other features.

We have proposed a series of protocol standards, including identity identifier protocol, multi-source entity verification protocol, user authorization protocol, distributed data exchange protocol etc. The implementation of various protocols is compatible with major protocol standards and systems at home and abroad. For instance, the identity identifier protocol is fully compatible with W3C's DID standard; the digital signature protocol supports ECDSA, SM2 and RSA and other algorithms; OAuth, UMA and other general authorization protocols are compatible with the distributed exchange system, which not only enables the architecture to meet the openness and standardization requirements, but also can support broader ecosystem cooperation and expansion.

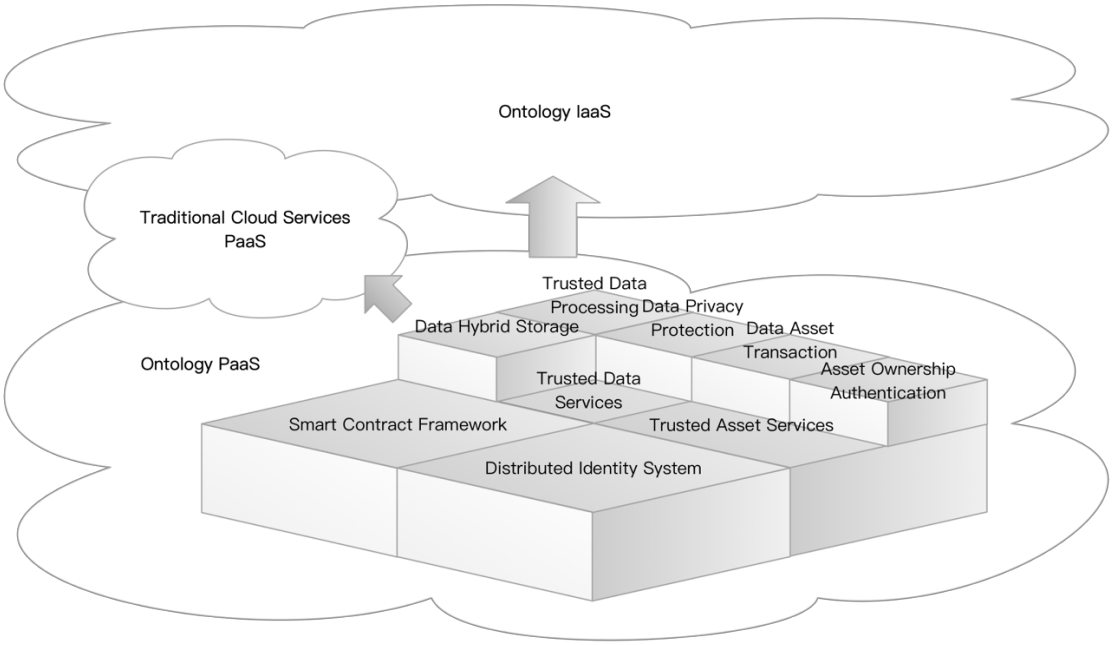

Figure: Service Platform Framework

Ontology will provide the “last mile” support for application services, with a series of application framework, including API, SDK and other function component, making it easier for application service provider in all industries to develop their own dApps. With Ontology’s support, application developers can directly provide distributed and decentralized services without the capability of developing distributed infrastructure.

2. Glossary

Ontology Distributed Ledger

One or more core public service chains built by Ontology's distributed ledger or blockchain framework, providing distributed ledger and smart contract system support to all type of services on Ontology.

Distributed Consistent Ledger

An incrementally modified data storage structure, maintained by nodes in a decentralized peer-to-peer network, featuring open data and tamper-proof historical data and providing trusted storage and smart contract support for Ontology.

Smart Contract

Executable codes recorded in the ledger that is executed by the smart contract engine running on ledgers nodes. The input and output of each execution can be recorded on the ledger.

Entity

Individuals who interact with others and are identified by ONT ID on Ontology.

ONT ID

ONT ID is a decentralized distributed identification protocol for identifying people, assets, things, and affairs. It is decentralized, easy to use, and can achieve self-management and privacy protection.

Verifiable Claim

A statement to confirm a claim made by one entity about another (including themselves.) The claim is accompanied by a digital signature that can be used by other entities for authentication.

Distributed Trust Framework

The core logic layer for Ontology to achieve distributed trust, which includes distributed identity identifier protocol, distributed trust model and distributed trust transfer system etc.

Multi-Source Verification

Refers to many different verifications covering various aspects of the same entity to create a multi-source verification.

Trust Anchor

An entity that is trusted by a certain group of entities, acting as a source for trust delivery chains and providing basic identity verification services for Ontology.

Anonymous Claim

An anonymous and non-connectable way to protect users' electronic credentials.

Identity Verification

A process to confirm the identity of the operator. Common authentication methods include passwords, credentials, biometrics and etc.

Asymmetric Cryptography

Also known as public key cryptography, is a cryptographic algorithm that uses pairs of keys. A key pair includes a public

key which is shared with all users and a private key which is kept secret and only known to the owner.

KYC

Know your customer. KYC is a business process that verifies client's identities and assesses its applicability, as well as identifying potential illegal risks in a business relationship.

DID

Decentralized identification that can be verified by cryptography and also self-govern.

3. Ontology Trust Framework

The Ontology blockchain network system offers four layers of services:

1. Trusted application system for end-users;
2. Define the precise roles of data providers and users, and provide a trusted data transmission solution that optimizes the way data circulates
3. Connect the upstream and downstream of the industrial chain and build a healthy business ecosystem of benign competition;
4. Trusted arbitration system that is legal and compliant and for industrial supervision.

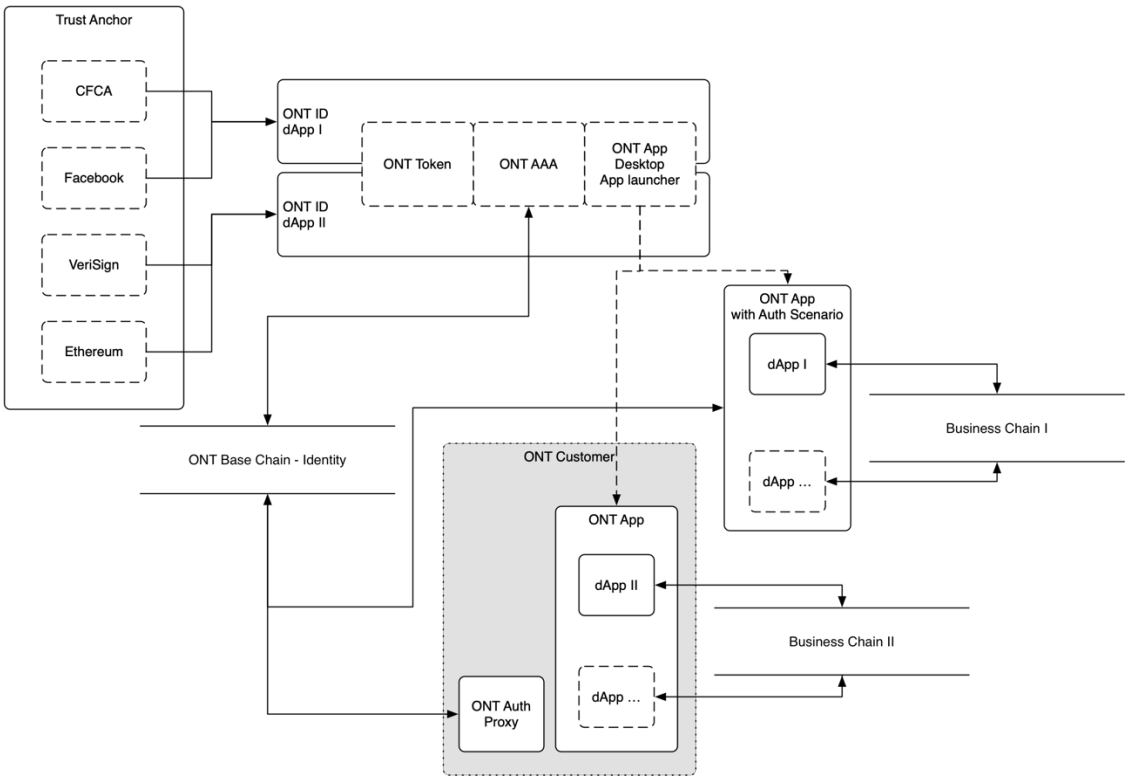

Figure: ONT ID Trust Framework

The core elements of the Ontology trust framework are as follows:

1. The multi-source trust system with a design endorsed by trust, featuring decentralized supervisory competitive trust, the distributed collaborative trust and a centralized strong trust anchor;
5. The Ontology decentralized identification (ONT ID) and a trusted claim system design based on people, assets, things, and affairs;
6. The ONT ID-based function chain that provides trusted services;
7. The blockchain service framework that meets different businesses' trusted security needs, and balances features and performance.

On this basis, we build the Ontology trust ecosystem based on information assets forms.

3.1. Ontology Identification Protocol

The Ontology identifier protocol (ONT ID) defines the process of putting data and data owner information on chain, the process of data processing and ownership transfer. The design of the protocol follows three principles:

1. Support integration of third party account system and storing it on blockchain, meeting the security and privacy needs of decentralization and user self-management;
8. Support data processing and data ownership transfer, ensuring both processes are traceable;
9. Support the decoupling of data ownership and data processing rights, making scenarios for data processing and ownership transfer more open and flexible.

The ONT ID protocol supports internet services, taking into account the current needs for Internet and Internet of Things (IoT). Considering the high-value of blockchain system, the ONT ID protocol also needs to support high-value data services.

To conclude, the ONT ID protocol supports the identification, recording and ownership authentication for people, things, assets, and affairs.

- The nature of people and things is ‘entity’, which refers to individuals, legal entities (organizations, enterprises, institutions etc.), things (mobile phones, automobiles, IoT devices etc.), and contents (articles, copyrights etc.) in the real world, while “identity” refers to its identity within the network. Ontology uses ONT ID to identify and manage the entities' network identities. On Ontology blockchain, one entity can have multiple identities, and there is no link between those identities.
- The nature of asset is the value of data information, usually defined by digital assets on-chain. It also refers to the data itself and can become one type of identity;
- Affairs describe the processes of data processing and ownership transfer. To meet open application scenarios, all data owners and processors are decoupled. This leads to the other two layers of identification, which are ownership identification and processing rights identification.

The ONT ID protocol contains entity identification, ownership identification and processing rights identification. These, combined with the digital asset identification, form the identification solution of the Ontology trust framework, where digital asset identification is designed with blockchain token.

Below figure shows the ONT ID solution:

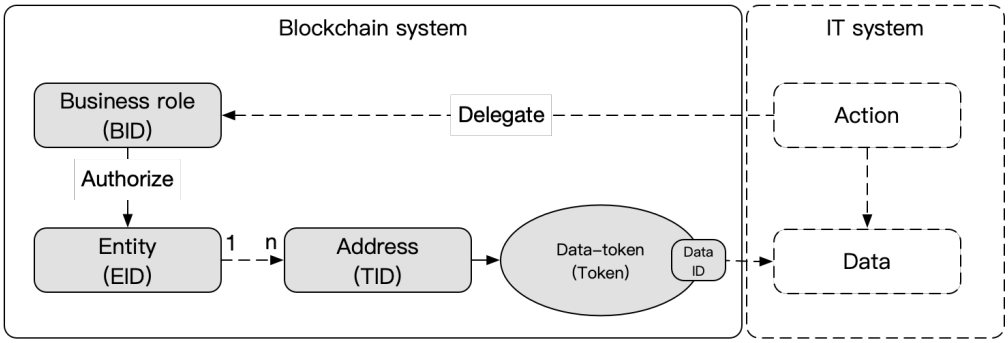

Figure: ONT ID Solution

Definition:

- Data ID: data identifier
- Data token: data accessibility identifier
- Token: blockchain token
- TID: token owner identifier (wallet)
- BID: business identifier
- EID: entity identifier

3.1.1. **Self-Sovereign**

Ontology uses digital signature technology to ensure that each entity manages their own identity. ONT ID is registered with the entity's public key to indicate its ownership. An ONT ID's use and its attributes need to be digitally signed by the owner. An entity can determine their own ONT ID's usage, bind a private key, and manage its attributes.

3.1.2. **Multi-Key Binding**

Ontology supports a variety of domestic and international digital signature algorithm standards, including RSA, ECDSA, and SM2.

Private keys bound to an ONT ID need to specify the algorithm used, and at the same time, ONT ID can bind several private keys to meet entity requirements in different application scenarios.

3.1.3. **Authorized Control**

The owner of the ONT ID may authorize other ONT IDs to exercise management rights over their ONT ID. For example, the attribute information corresponding to the ONT ID may be modified, or another private keys can be bound to an ONT ID if the original key is lost. ONT ID supports fine-grained permission management for each attribute and multiple access controls such as “AND”, “OR”, “m of the n”.

3.2. Trust Network

The Ontology trust network refers to the trust network formed between entities that meet the requirements of the Ontology identifiers. The network is composed of trust anchors, verifiable claims, and multi-source authentication protocol. The Ontology reputation system is based on the Ontology trust network.

3.2.1. **Trust Model & Trust Anchor**

The trust model provides support for trusted scenarios which mainly serve as trusted channels for business cooperation between trustees and verifiers. The trust model is composed of trustors, trustees, and verifiers, where a trustor endorses a trustee, then the trustee can pass the verification of a verifier that trusts the trustor.

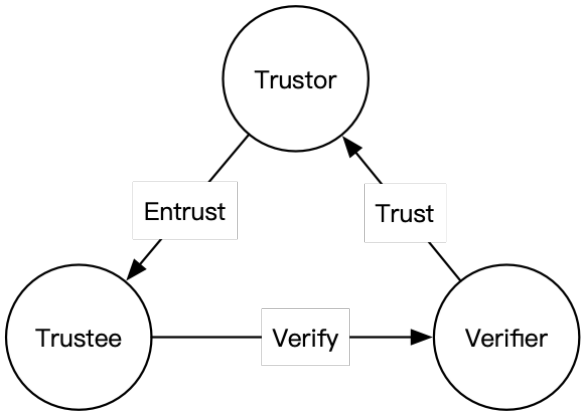

Figure: Trust Model

Under this model, the trustor is named “trust anchor”, through which “verifiers” locate trust and trust “trustees” with the trust certificate of the trust anchors.

Under this model, a trust anchor is established by one entity or a group of specific entities, and thus forms the foundation of trust relationship among entities. The trust anchor specifies the entities it trusts, and the other entities can in turn specify other entities they trust. Thus, with a trust anchor as the source, a trust delivery tree forms. In the tree, each node has a path to the trust anchor, which is the node’s trust chain. When interacting with nodes from the tree, an entity that acknowledges the trust anchor can know its credibility by verifying the anchor’s trust chains.

Ontology's trust model generates trust between entities using both centralized and decentralized trust models. Different trust models can be used according to specific scenarios to meet different needs.

3.2.1.1. Centralized Trust Model

As the most widely used trust system today, PKI is a centralized trust model. To become a trust anchor a user must first apply for a digital certificate. After approving the application, the certification center

writes its identity information and public key into the digital certificate, and then adds the digital signature of the certification center. The digital certificate issued by the certificate authority authenticates the binding between the user's identity and the public key. Anyone can use the public key of the certification center to verify the authenticity of the certificate, and then use the public key in the certificate to verify the user's signature and confirm its identity. At the same time, users who have digital certificates can also issue digital certificates to other users as subordinate certifiers, and the validity of the digital certificates issued by them is guaranteed by the certification center. In the PKI model every participant must unconditionally trust the certificate authority, and the trust relationship is passed from the certificate authority layer by layer between entities though digital signatures.

The centralized trust model has many advantages. The strict method of trust transfer and the clear trust and non-trust boundary are good features in many scenarios and can solve many problems. However, there are certain disadvantages to the centralized trust model. The dependence on the centralized node may be unsuitable for complex trust relationships, as well as for in cases where there are higher demands for unconditional trust anchor, honesty, and security. This method of relying on the centralized node can severely limit application flexibility.

3.2.1.2. Decentralized Trust Model

In addition to relying on specific centralized entities to build trust, entities can also build equally strong trust by themselves. Trust transfer is achieved through mutual authentication between entities.

Entities will have higher credibility if they are authenticated by more entities – especially if those other entities have high credibility.

The decentralized trust model is a diverse trust model that supports multiple trust sources and trust dimensions. Under different scenarios different trust assessment methods can be used to evaluate the trust of entities. It is because of this high degree of flexibility that the model has a wide range of applications in real life.

3.2.2. **Verifiable Claim**

Verifiable claims are used to prove certain attributes of an entity. They can be stored and transmitted as data units and verified by any entity. A claim includes metadata, claim content, and the issuer's signature, while the content can be any data.

3.2.2.1. **Life Cycle**

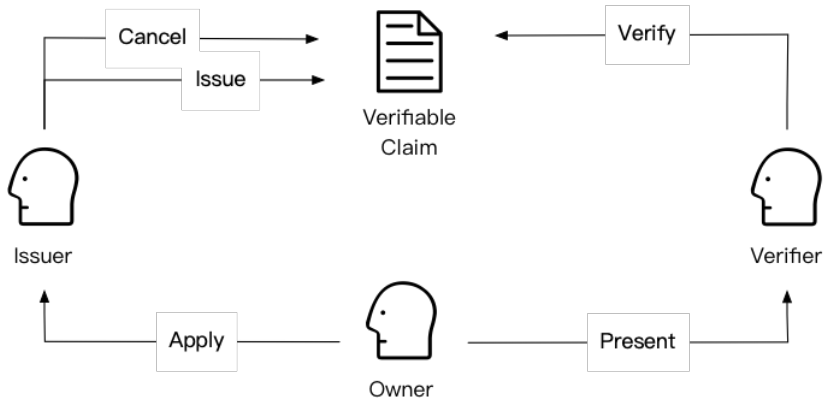

Figure: Verifiable Claim Lifecycle

Entities associated with a verifiable claim fall into three categories: trustor, trustee, and verifier. The life cycle of a verifiable claim includes the following five operations:

- Issuance: Any entity can issue a verifiable claim of an attribute of another entity. For example, a school may give a student their

transcript or a bank may give a client a statement of their assets by issuing a verifiable claim. When a verifiable claim is used a validity period can be set. When the validity period has passed the claim will automatically expire.

- Storage: Verifiable claims can be issued as either public claims or private claims. Public claims are stored in a distributed ledger on Ontology, whereas private claims are typically stored on the entity's client and managed by the entity itself.
- Presenting: The owner of the verifiable claim can choose to whom the claim is made public and which information is shown without affecting the integrity of the claim.
- Verification: The verification of the verifiable claim does not need to interact with the issuer of the claim, it only needs to use the issuer's ONT ID to obtain the public key information from Ontology's distributed ledger. It can then use the public key to verify the digital signature of the claim.
- Cancellation: The issuer of the verifiable claim can cancel their claim before the expiry date. The cancelled claim will not be able to be validated.

3.2.2.2. Anonymous Claim

Normally, the claim owner exposes the full content of the claim to the verifier when it makes a claim. However, in some scenarios the claim owner may not want to expose certain content of the claim to the verifier. In light of this, Ontology offers anonymous verifiable claim technology to protect the privacy of its users.

Anonymous Claim technology solves the problem of hiding the holder's information during the process of issuing and presenting a

claim. In the anonymous claim protocol an entity receives two verifications of their claim from two different verifiers. Even if the two verifiers wanted to conspire together to leak the information they hold, they would not be able to verify whether the information they received is from the same entity. When making an anonymous claim the issuer does not need to provide the original claim to the verifier, they only need to provide a zero-knowledge proof. The verifier can verify the authenticity of the claim by running a validation algorithm with the issuer's public key, certificate, and an assertion of the attribute values contained in the certificate, e.g. “age > 18” AND “resident of Singapore”.

An anonymous claim contains both public and cryptographic information. The public information includes all the attributes of the anonymous claim, consisting of three parts: the name of the attribute, the type of the attribute, and the value of the attribute. Attributes support a variety of data types, such as strings, integers, dates, and enumeration types. The cryptographic information mainly includes the owner's own master key and the issuer's public information digital signature.

During the presentation of the anonymous verifiable claim the owner proves to the third party verifier

that he owns an anonymous claim from an issuer. They can selectively expose some attribute values and hide other attribute values. In addition, they can prove that some hidden attributes satisfy certain logical assertions.

3.2.3. **Multi-Source Authentication Protocol**

Multi-source authentication is different from existing single-factor authentication systems. Ontology can provide entities with multi-source authentication systems which integrate the authentication of external identity trust sources and the endorsement of entities on Ontology. The multi-source authentication protocol includes the following two modes:

- External trust source certification: Ontology binds ONT ID to an external trust source with a self-signed verifiable claim. Any entity can verify the identity of an entity by verifying the external trust source bound to the ONT ID. The trustworthiness of an entity's authentication is determined by the trustworthiness of external trust source bound to the ONT ID;
- Authentication between Ontology entities: Entities in Ontology can also authenticate each other by issuing claims between themselves.

3.2.3.1. **External Trust Source Authentication**

External trust source authentication supports self-import and trust-anchor-import.

1. Self-Import

Users bind real-world trust through social media, bank UKEY signature etc., which leverages the existing trust in the real world. Through self-import, an attestation address of an external trust source is added on Ontology and a verifiable claim implementation is provided in that address, including:

- Claim creation and expiration time

- Claim content: including the claim type, ONT ID, social media platform, social media username, etc.
- Signature: a designated public key that must be in the public key list in the ONT ID.

When a third party needs to verify the user's external identity, it first reads the attestation address of the user's trust source on Ontology, then goes to the address to obtain a verifiable claim, and finally verifies the claim.

10. Importing through Trust Anchors

Trust anchors abide by Ontology's standards and are formed by trustors trusted by verifiers. Trust anchors use their own authentication methods to authenticate entities and issue verifiable claims to the authenticated entities.

The claims do not need to contain the identity information of the authenticated entities; only the ONT ID and the authentication service are recorded, and the authentication result can be provided. The authentication model is as follows:

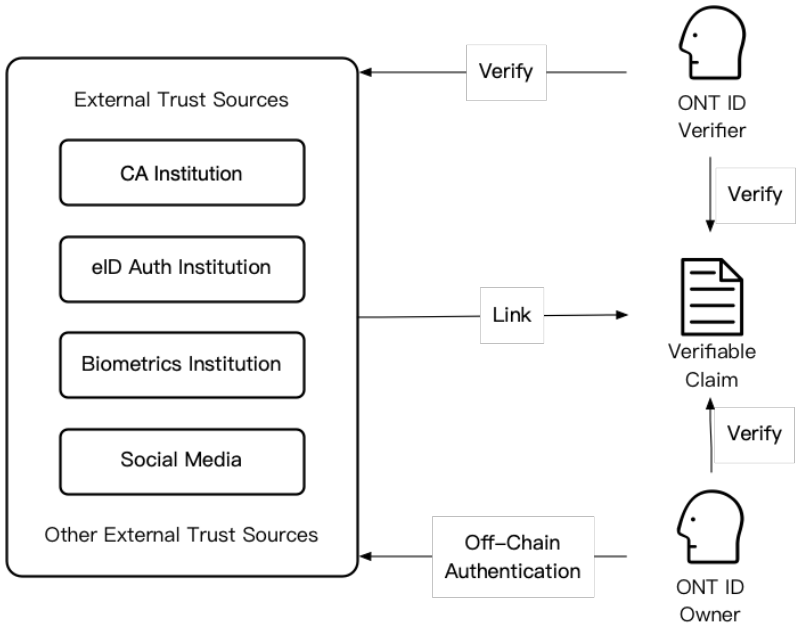

Figure: External Trust Anchor Authentication

3.2.3.2. Identity Authentication between Ontology Entities

Entities on Ontology can also authenticate identity through entities that have passed identity authentication (from an external trust source) on Ontology. As shown in Figure 6.2, users can not only authenticate their identity through entities like schools and banks, but also through individual methods.

Due to the openness of verifiable claims, any entity on Ontology can make a claim about anything regarding another entity. This takes identity authentication on Ontology far beyond the traditional concept of identity authentication. This multi-faceted and multi-dimensional authentication system is far more accurate and comprehensive than traditional systems.

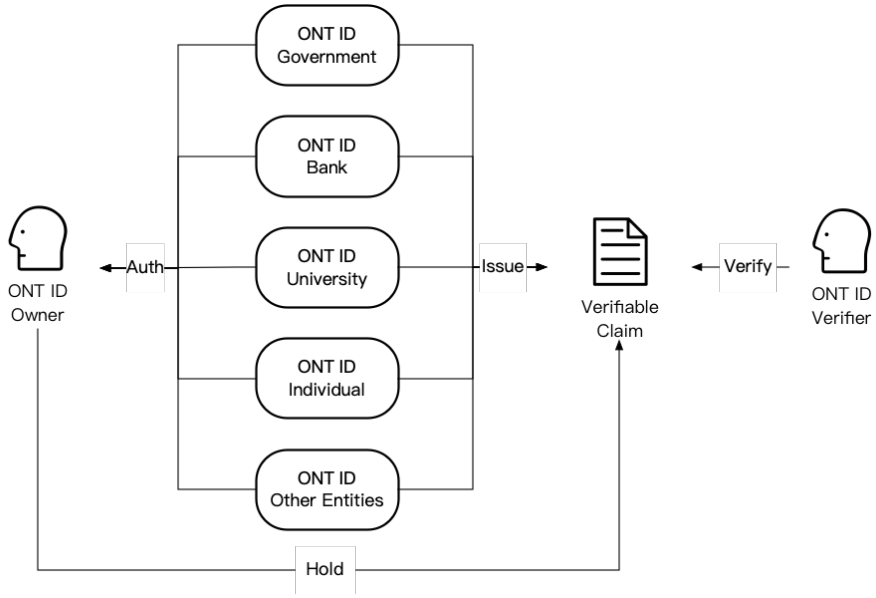

Figure: Identity Verification between Entities

3.2.4. **Distributed Reputation System**

The distributed reputation system is an important part in the Ontology trust network, which integrates the Ontology trust network and the Ontology business application. On the one hand, a trustee evaluates the reputation of a verifier to draw traffic for the verifier, which will improve the user interaction experience of an application to better serve users. On the other hand, users utilize different business applications, and as the trustor, the application provides endorsement for the trustee. Good reputation will help users receive better services, and by continuously enhancing the reputation in the Ontology ecosystem, it will also improve user quality in the entire application ecosystem.

4. Distributed Data Exchange Framework

The Distributed Data Exchange Framework (DDXF) realizes decentralized transaction, exchange and collaboration between entity resources and on-chain assets via consistent ledger, smart contract, cryptography and other technologies.

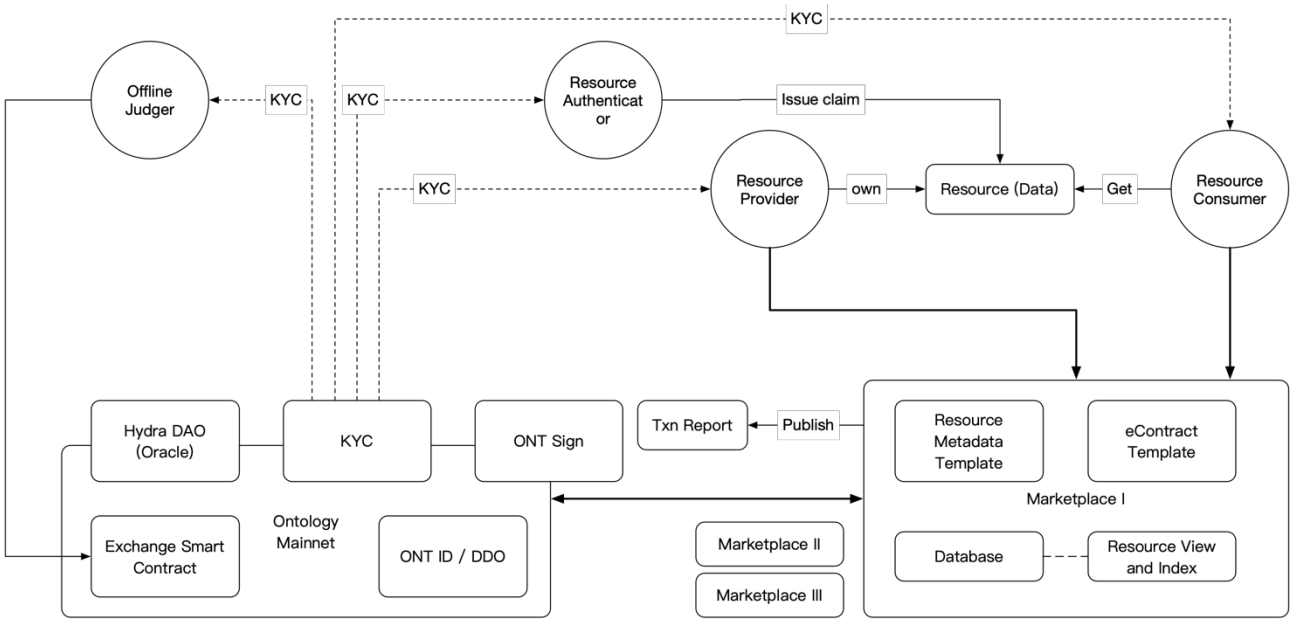

Figure: DDXF

Based on DDXF, we can create a platform that provides on-chain ownership authentication and resource circulation, exchanges resources for ONG, OEP-4 and other digital assets, or exchanges resources. The resources DDXF supports include digital resources and entity resources. DDXF also supports digital resource circulation and entity resource circulation. The on-chain circulation of resources

includes the circulation of resource ownership, right of use or other rights. As for off-chain entity resources, DDXF supports off-chain settlement by introducing electronic contract while taking into account the compliance of off-chain behaviors, thus ensuring the security and consistency of both on-chain and off-chain behaviors.

4.1. Ontology Resource Assetization

Resource assetization refers to binding resources and the Ontology identity system onto the chain to receive the ONT ID of the resources after digitizing and standardizing off-chain resources, then tokenizing the corresponding rights of the resources so that resources are fully assetized. DDXF uses resource token to achieve collaboration and exchange on the chain.

Tokens are created, burned, and distributed based on the characteristics of resources' rights, including fungible, non-fungible, and partially fungible tokens. Combined with ONT ID authorization management, the transfer process of the resource rights is traceable.

Tokens can be traded. On the basis of asset assetization, the Ontology solution involves the value quantification and transaction of token by describing the meta information of resources.

Ontology uses the DToken protocol to assetize resources. DToken is composed of a series of different functional protocols, including resource meta information extraction, defined meta information template, resource tokenization standards, DToken value binding, DToken ownership transfer, etc. In practice, users are free to select modules that suit them to encapsulate business according to their business scenarios.

4.2. Distributed Data Exchange Protocol

Ontology proposes a distributed data exchange protocol and expands its application scenarios to all valuable resources. The protocol has defined a full set of protocol standards for data interaction between entities targeted at existing pain points of today's centralized data exchanges, such as data cache, unauthorized private data, and unprotected data copyright.

To ensure the security of data interaction and protect the interests of interacting parties, the protocol has defined generic interaction scenarios and the precise roles of the interacting parties, and also specified the behaviors of the roles along with the open interface design in the architecture, thus ensuring the consistency and security of interaction, sharing, and exchange between off-chain resources and on-chain assets.

4.2.1. **Role Definition**

The roles in the distributed data exchange protocol mainly include:

- Resource Provider (RP): Entities that own resources and release them to the market to obtain certain benefits from those resources through a pricing system. There are many kinds of these entities, such as data owners, computing power owners, data collection platforms, and data custodians with a certain level of authority etc.
- Resource Consumer (RC): It is the counterparty of the resource provider. It is an entity that needs resources from the provider. They obtain (partial) rights to the resource from a RP and pay a certain fee for it;

- Resource Authenticator (RA): A third party with certain authority that has its own resource quality certification system, where they can provide resources or RPs with some authentication and enhancement resources, or provide the credibility for RPs;
- Off-chain Jury (OJ): An off-chain arbitration jury that is acknowledged by both RP and RC in a resource transaction. Disputes that occur off-chain will be adjudicated by OJ;
- Marketplace (MP): A belt that connects RPs and RCs. It stores resources' meta information and provides the resources with flexible display and fast retrieval services for transaction fees. Each MP can provide flexible and scalable services according to its transaction characteristics, such as offering meta information template and electronic contract template that can be used by both sides of the transaction for resolving off-chain disputes. In addition to the pricing system for resource transaction, MP has a resource transaction information disclosure system, so it can disclose transaction information to the public or regulators.

4.2.2. **User Authorization mechanism**

In the data exchange system, since transaction data need to be authorized by resource owners, the authorization process fully abides by the user authorization protocol.

4.2.3. **Data exchange process**

1. Resource Preparation:
    a. (Optional) RP requires RA to authenticate the resource to be released;

b. For resources that will be released on the chain, RP will create an ONT ID and corresponding DDO information which serves as resource's mapping on the chain;

c. Confirming the exact pricing method according to the pricing system provided by MP;

d. Creating respective resource meta information of the resource according to its meta information template provided by MP;

2. Resource Release:
    a. RP submits resource's ONT ID, meta information and its pricing method to MP;
    b. MP retrieves corresponding information of the resource from the chain and its own database;
    c. MP displays the resource, enabling RC to quickly retrieve resources with the meta information.
3. Resource Transaction:

    a. RC quickly retrieves and finds the resource they need according to the resource meta information in MP and confirms the resource they want to transact;

    b. RP and RC materialize their electronic transaction contract according to MP's electronic contract template, appoint an OJ and sign the electronic contract, then record everything in the smart transaction contract. Depending on MP or contract requirements, RP and RC might respectively be required to stake a certain amount of ONG into the smart contract for dispute resolution and post-transaction division of profit;

c. RP creates DToken according to the electronic contract and authorizes a right, such as (partial) ownership or right of use of a resource to RC;

d. When transaction is in the lock-up period, RP will use DToken to exchange for the disposition right of the resource. If a transaction dispute occurs during the lock-up period, both parties have to provide on-chain or off-chain proof. OJ or HydraDAO will then intervene and adjudicate the dispute based on the off-chain proof;

4. Division of Profit:
    a. Once the lock-up period ends profit will be divided according to the transaction result. OJ or HydraDAO's ruling of a dispute might trigger an early division of profit;
5. Post-transaction Review:
    a. RP and RC review each other, and the review can be of the resources or users;

5. Ontology Application Framework

The Ontology application framework is based on the Ontology trust framework and the Ontology distributed data exchange framework.

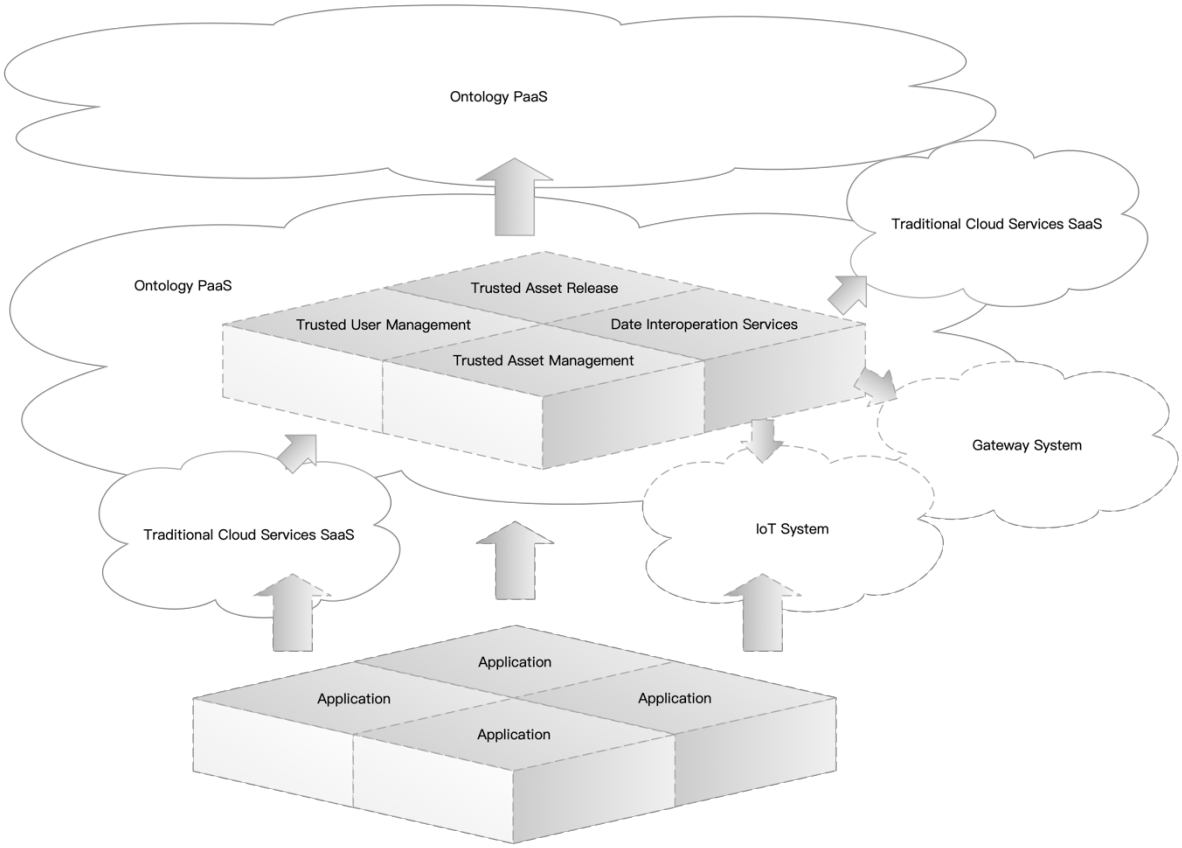

Figure: Ontology Application framework

Ontology's application framework provides a rich set of application protocols and modules that enable dApp developers to quickly build decentralized applications without having to understand the complexities of the underlying distributed ledger. The framework has a high degree of scalability and can be expanded according to the application scenarios.

Figure 7.1 is the application framework model, which shows how dApps interact with Ontology through its application framework to achieve decentralized trust:

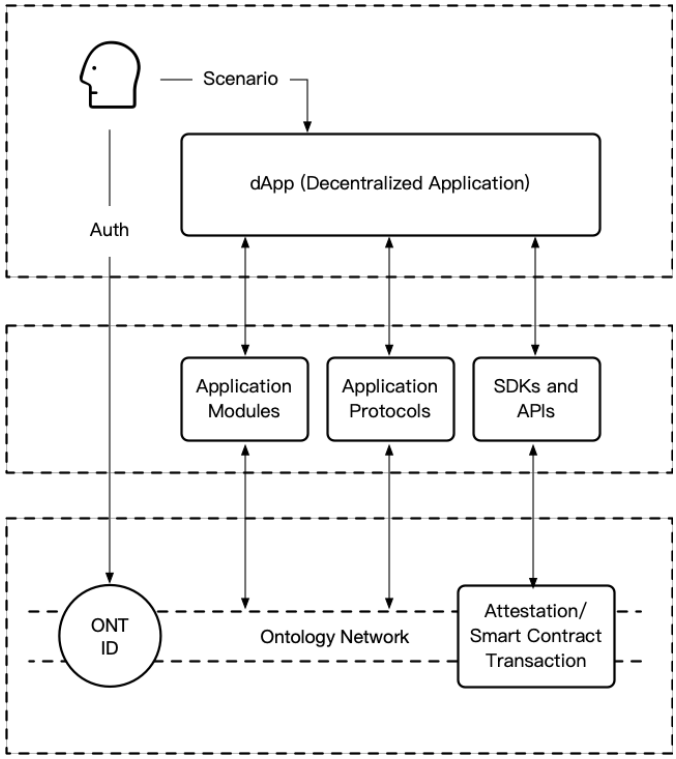

Figure: Application Framework Model

Ontology realizes distributed trust through decentralized identity system, attestation, and smart contract transaction; the framework enables the upper-layer scenarios to make better use of Ontology through application modules, application protocols, SDKs, and APIs. Business dApps focus on business scenario development and user services.

5.1. Ontology Application Access

Base on the Ontology application framework, Ontology provides trusted asset release, trusted user management, trusted asset management, and data inter-operation services to support

application access. Ontology ecosystem partners can prepare solutions by secondary encapsulation of these four modules to provide services for the Ontology application ecosystem.

Ontology offers trusted application solutions that support business application access to the Ontology trusted ecosystem. Trusted business applications can help build an application market, enabling end-users to select the business applications they want. Similar services can compete with each other in a healthy manner in the trusted ecosystem, promoting the development of businesses and the application market. The distributed reputation system in the Ontology ecosystem is an essential part of the application market.

6. Postscript

This White Paper introduces the technologies and protocols under the Ontology trust framework and will be subject to updates as more applications are being supported.

Ontology is dedicated to building an open, collaborative, and innovative trust application ecosystem. The Ontology team welcomes developers from around the world to join us and help us develop the Ontology application ecosystem.

Contact Us

Email:
contact@ont.io

Telegram:
OntologyNetwork

Twitter:
OntologyNetwork

Facebook:
ONTnetwork

Reddit:
OntologyNetwork

Discord:
https://discord.gg/vKRdcct

Medium:
OntologyNetwork

LinkedIn:
Ontology