DataObjects – Transforming Data Management Through Digital Claims, Verified Ownership, and Secure Agreements

Ian Kelly ***Ian@idobjects.io*** *February 2025* ***Version**: 1.0*

Patent Pending

Abstract

The increasing complexity of data systems demands new methods to ensure data ownership, integrity, and security. This paper introduces **DataObjects**, a novel data structure that enables persistent tracking, validation, and verification of data ownership and history across systems. The **DataObject** paradigm uses cryptographic methods to confirm data integrity without exposing its contents, allowing secure, trustable, and verifiable interactions. The technology supports the creation of **Digital Identities** (**IDObjects**), and **Digital Claims**, which allow individuals and organizations to assert ownership and confirm facts without revealing sensitive information and the extension of Smart Contracts to establish **Digital Agreements** via governed and auditable relationships between **Digital Identities**. By enhancing data traceability and security, this invention opens the door for new applications in smart contracts, data governance, and decentralized systems**.**

Table of Contents

Data Assertions

Assertion #0	*Data is the observable product of a change in state*
Assertion #1	*Data is property and can be owned without being possessed*
Assertion #2	*Data has ownership and provenance*
Assertion #3	*If data can be verified, it can be a claim*
Assertion #4	*One can use digital claims to enter into a secure digital interaction without revealing the content of digital claims or providing excessive personal information*
Assertion #5	*One can be assured of secure connectivity between people using the terms of a digital agreement*
Assertion #6	*If provenance and identity are assured, data can be open and secure*
Assertion #7	*If I control the usage of my data, any processing on that data is no longer "on my behalf", it is "as if" I am executing the processing.*
Assertion #8	*If my digital activity is secure and repeatable, the collection of these digital agreements and digital claims becomes my verifiable online identity, even if I am anonymous, pseudonymous, or acting on behalf of an organization.*

Introduction

In this digital era, data, personal or otherwise, is provided by users at an unprecedented rate and monetized by the platforms they interact with; giving the user no control over their data once provided. This data movement and asymmetrical exchange does not permit the owner or producer of the data any ability to control, correct, or redact data they provide in any meaningful way outside of hard to enforce Data Privacy laws such as GDPR and CCPA. The user is at the mercy of the data consumer and processor and their rights to their data are limited.

Data is created constantly and moves across multiple systems. Ensuring the origin, ownership, and integrity of data across these systems has been a persistent challenge. The traditional model of data ownership, storage, and transfer lacks a robust mechanism for validating the history and authenticity of data as it is shared between different custodians, platforms, and organizations.

The **DataObject** is a new data structure designed to overcome this limitation. It encapsulates the context, history (provenance), and ownership of data, enabling data owners/producers and systems to verify the integrity and ownership of data in a secure, traceable manner. Unlike conventional data structures, DataObjects do not reveal the underlying data but still allow for validation through cryptographic means.

Overview

Data is a type of property that we create every day. We give it away, and others profit from it. To control and be accountable for our data, we need a way to manage its creation, use, and ownership.

A DataObject is an immutable mathematical construct that represents a piece of data with associated metadata, such as its type, operation, history, and logic. DataObjects are permanent and unchangeable, but they can provide predictable responses to questions about their state and contents.

DataObjects have unique IDs that allow computer programs to call them directly. They can be used to represent any type of collection, set, or sequence, and their data can be in various formats, including numbers, letters, media, and algorithms.

DataObject owners can control access to the underlying logic used to create the data, while still allowing it to be executed. A record of every execution is stored in an immutable public log.

Digital Identities (IDObjects) are a concept that represent individuals as unique labels or data that they can prove belong to them. They can be linked to anonymous IDs,

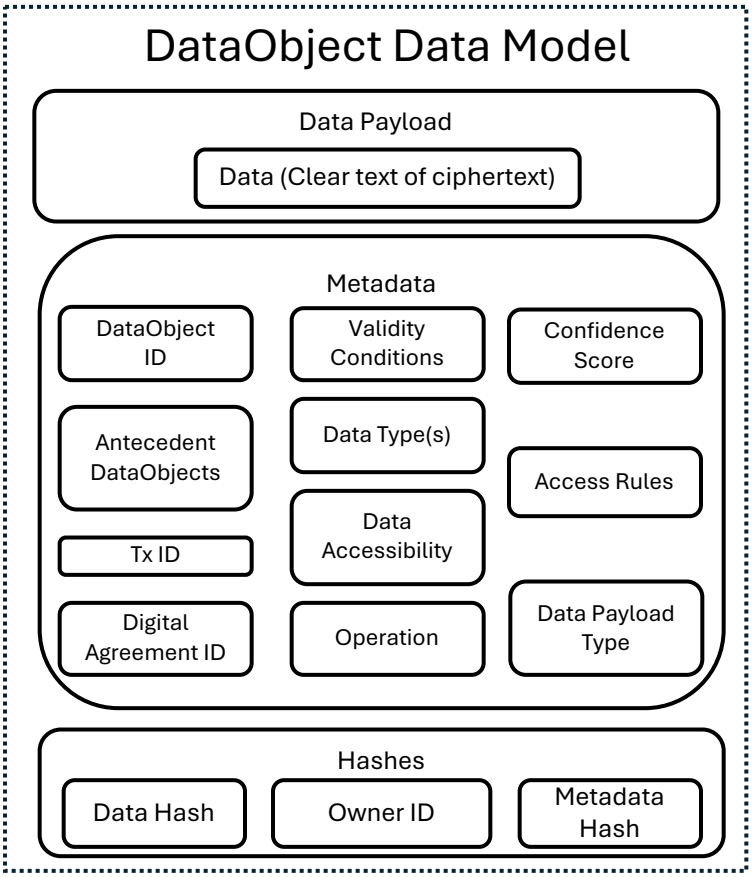
organizations, pseudonyms, or real names, and can be derived from other Digital Identities belonging to the same person.

Digital Claims are specialized DataObjects that answer specific questions in a way that doesn't reveal knowledge but proves ownership. They can be supported by external authoritative data sources, such as government agencies, which digitally sign and assure the validity of the claim.

The relationships between data and identities can be managed through Digital Agreements, which rely on internal terms and conditions as well as Digital Claims to ensure their validity

Specification

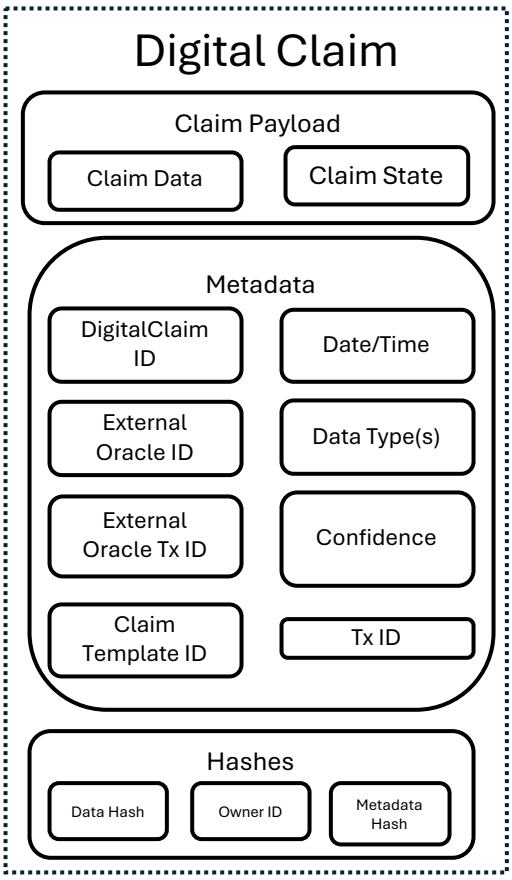
The **DataObject** is a data structure that encapsulates details of the owner of the data, the data type, the operation that created it, when it was created, what data it relied upon to be created, methods to view and validate the data, a way to reference the data (and preceding operations and data), a set of conditions under which the validity of the data's state is reliable which can apply to data or viewer/checker of data, a process by which any access or viewing of the data structure is immutably logged, a reference (if applicable) to other data in the series, sequence, or set, and a probabilistic confidence in the data.



DataObjects implement the rules and structures required to bind data to its originating process, the data it relied upon for processing, the function or algorithm used to create it, the owner or producer of that data, an immutable integrity that the data is unaltered that makes the validation of that data possible with measurable confidence and cryptographic congruence a simple task not requiring the revealing the underlying data itself.

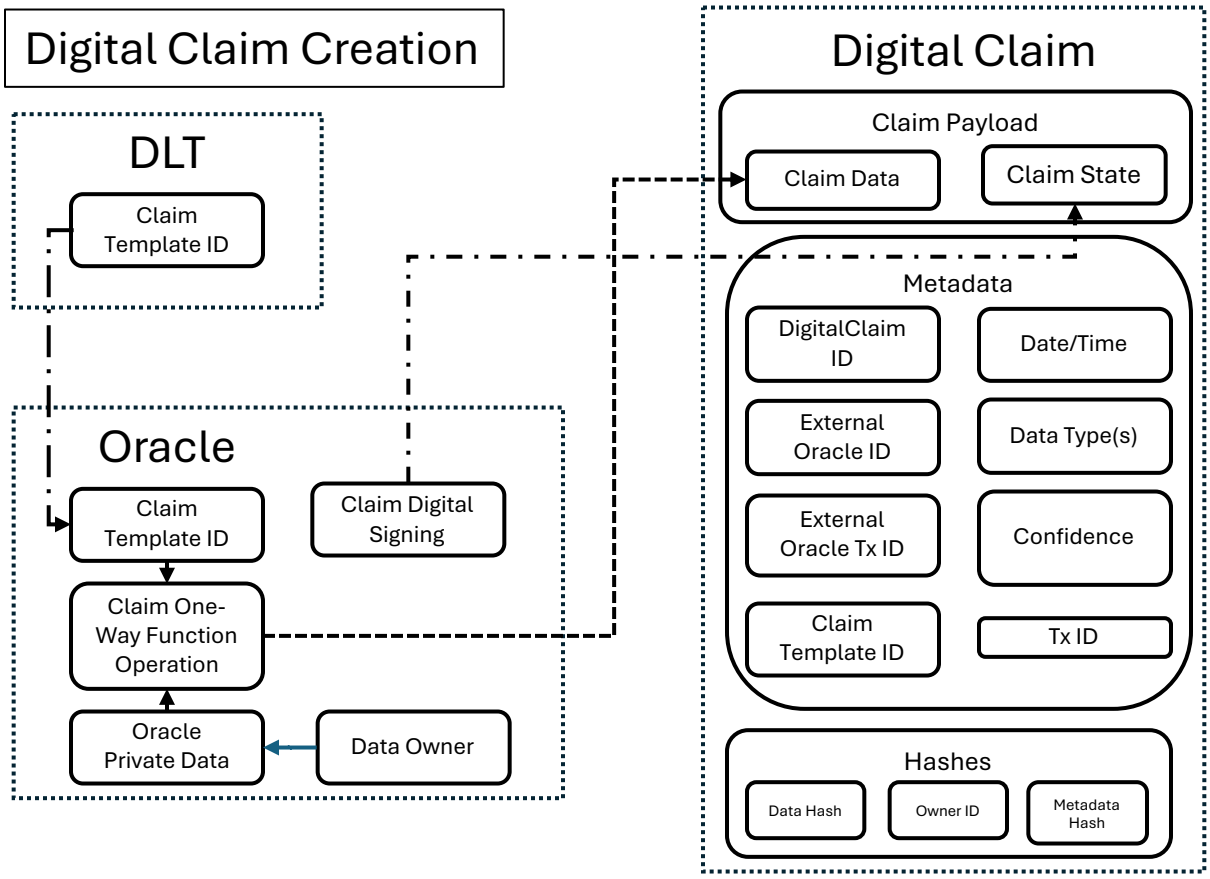
This data structure can be referenced, asserted to by a natural person (via a Digital ID detailed below) to prove ownership, interrogated for its state, verified for its integrity, and validated for mathematical accuracy.

Further, this data structure binds data to its owner in a way that the validity of the owner can be checked without revealing the name or identifying features of its owner. There is a one-way relationship from owner to data whereby the owner can assert ownership without revealing their identity but proving *only* they could be the owner of the data and for a data verifier, who is not the owner, can be assured that an owner exists, is who they claim to be, and assures the integrity and validity of the data.

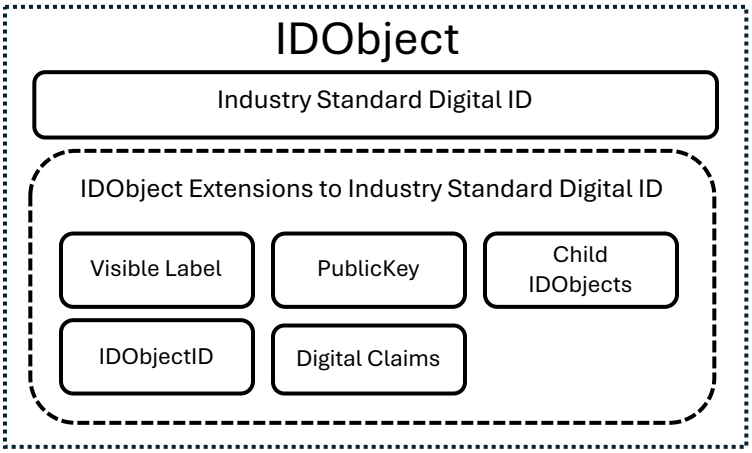


The data this structure describes and contains can be any machine or human readable data; binary, text, numbers, computer code/operations/algorithms, images, video, or cipher text. This data structure can also reference another data object (using the same data structure) providing a chain of data or operations who's state, data validity, and antecedents can be interrogated allowing the data structure to "inherit" other data/operations by reference with calculable confidence and without having to rerun the operation creating the antecedents data or operation; thus making the validation of the output of a data operation that uses antecedents able to be validated by reliance on that antecedents known validity. The invention makes possible the creation of a public and verifiable web of data.

The data structure can be assured by an external/real-world oracle system or institution (authoritative data source such as a governmental agency or trusted party). When this feature is activated, the data structure, when referenced or interrogated, produces cryptographically verifiable output that the data's state is correct by the execution of a public and immutable function on the core data that could only produce specific output. This feature allows the data structure to be used as a verifiable digital claim whereby a condition's state is known.

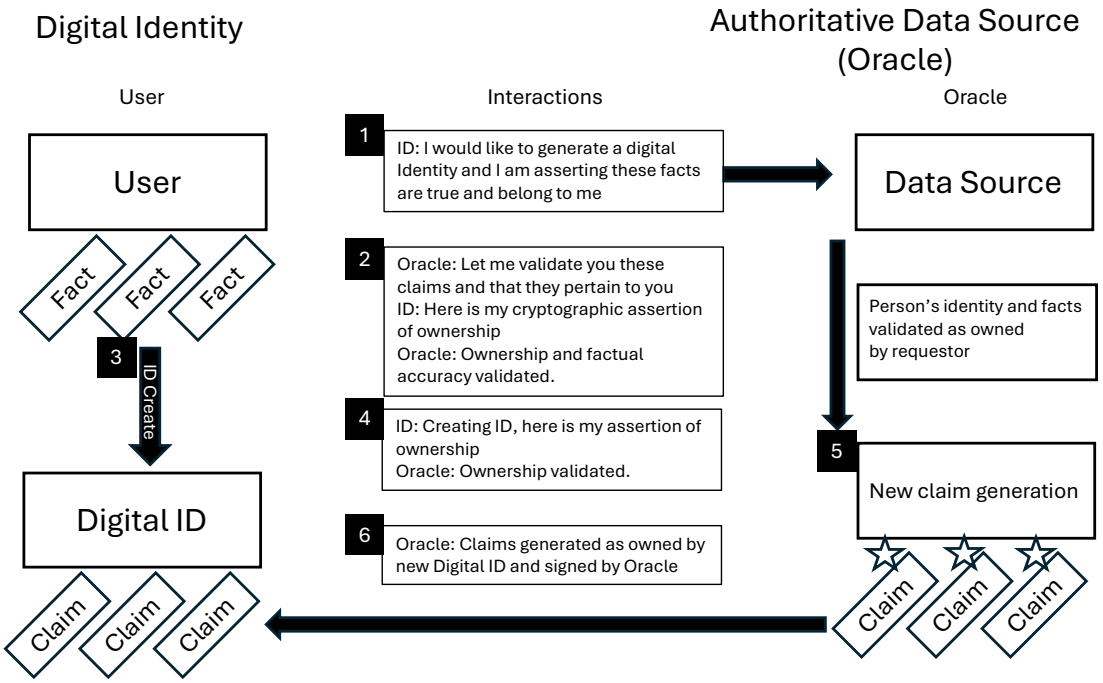


The core data structure necessarily contains ownership details because of a one-way connection to a digital identity. For example, the data object structure for a piece of data could contain a SHA256 hash (or a suitable key length to protect from Quantum guessing) of the UUID of the digital identity that claims (and can in a cryptographically congruent manner) assert ownership of it. This digital identity represents a real-world person or organization. The digital identity points to verifiable digital claims as cryptographic proof of validity. Digital IDs are thus built upon digital claims that are testable, reliable, and dependent on the validity of underlying claims.



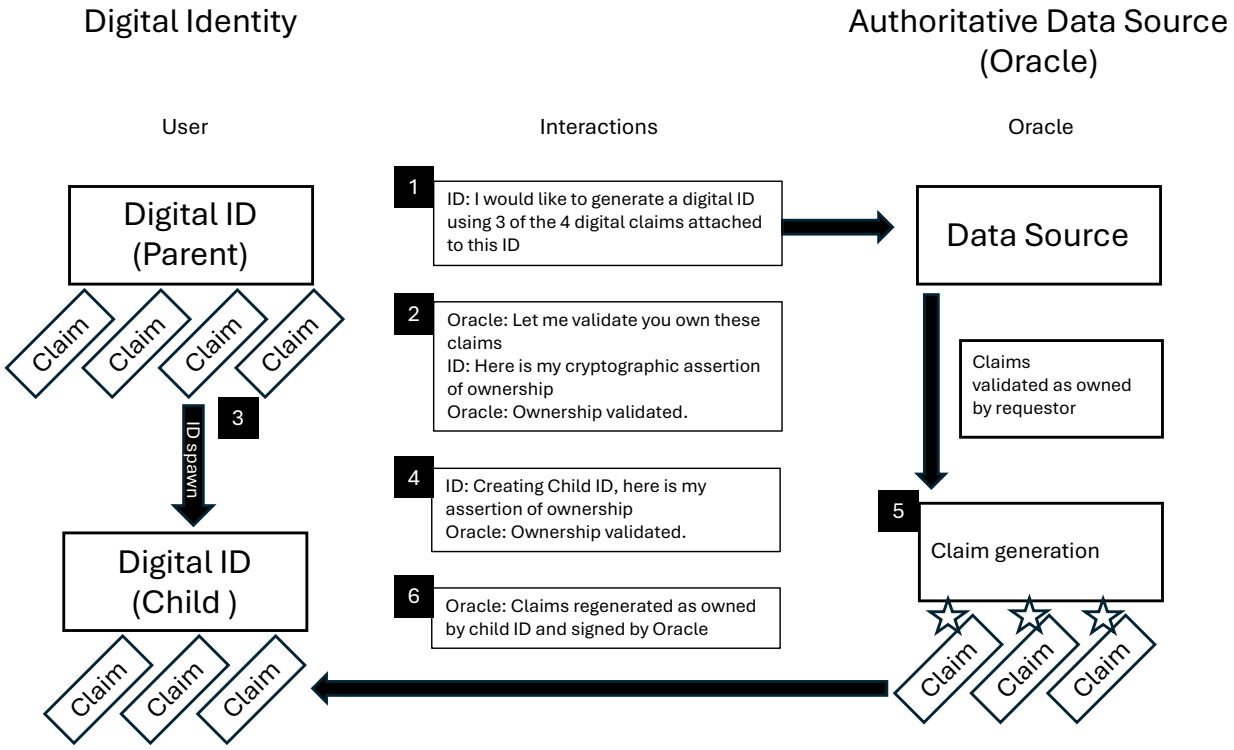
Further, these digital identities can create child digital identities, validated by the parent's verifiable digital claims, that can be used in digital interactions to prove a human/organization is valid but without necessarily revealing the identity of the parent. Such child identities can be real name, pseudonymous, anonymous, or organizational. Parent identities can assert ownership of the child identities without revealing the parent's identity and child identities do not allow non-parent identities or processes to derive the parent's identity from the child's identity.

Figure 1: Digital ID Creation



1. Request that Oracle validate person's identity and claimed facts
2. Oracle validates identity and facts based on their own authoritative records
3. User creates a Digital ID
4. Digital ID provides Oracle the ID name and a cryptographic assertion of ownership
5. Oracle validates facts are true and belong to requestor based on their records
6. Oracle signs new claims and provides to parent ID to attach child ID

Figure 2: Digital ID Child Creation



All parent identities of the spawned child ID can read data written by child identities even if encrypted.

By binding data to its origin/context/predecessors and owners, digital identities can enter into digital agreements with other digital identities to produce, share, use, transact, or interact with measurable confidence by specifying (such as in a DLT smart contract) the terms and conditions of such interactions. These agreements can stipulate which digital identities' underlying verifiable digital claims must/could/should (or not) have a specific state, the terms and conditions of the agreement, testable, trustable, and auditable output, actions, and expectations of the agreement, ownership rights of any data produced by the agreement, access control on who can view the agreement produced data, remedies for non-compliance, agreement duration, and the ability for the auditing of the agreement by a party not privy to the data the agreement produces, owns, or claims. This basis of a digital agreement is not claimed as original to this invention but extends the concept of smart contracts as implemented on blockchain technology, such as Ethereum.

Features of DataObjects:

1. Persistent Data Ownership and Validation

DataObjects permanently link data to its origin, ensuring that the ownership and creation context can be verified at any point. Ownership claims are cryptographically bound to the data without revealing the identity of the owner. This creates a secure and privacy-preserving system for data transactions.

2. Immutability and Integrity

DataObjects are immutable once created. This ensures that the integrity of the data cannot be tampered with after its creation. Any attempt to modify a DataObject would make its hash and DLT entry not match the actual and invalidate it. Accesses of the DataObject are publicly logged, ensuring traceability.

3. Digital Claims and Identity Management

A key extension of the DataObject framework is **Digital Claims**, which allow users to prove assertions (e.g., age, citizenship, or identity) without revealing sensitive information. Digital Claims are built into Digital Identities, which are derived from user-controlled **IDObjects**. These can create child identities, which can be used pseudonymously, anonymously, or organizationally while still verifiable as linked to a human. This feature protects users from interacting with bots pretending to be real people.

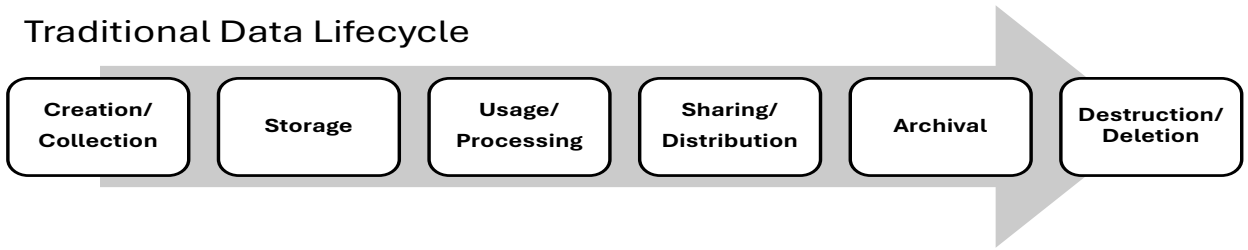
4. Cryptographic Validation Without Data Exposure

Using cryptographic techniques like encryption and zero-knowledge proofs, DataObjects can validate data without exposing the underlying content. This makes them ideal for use in systems that require verifiable but confidential data, such as financial transactions or healthcare data exchanges.

5. Updating of Data Lifecycle

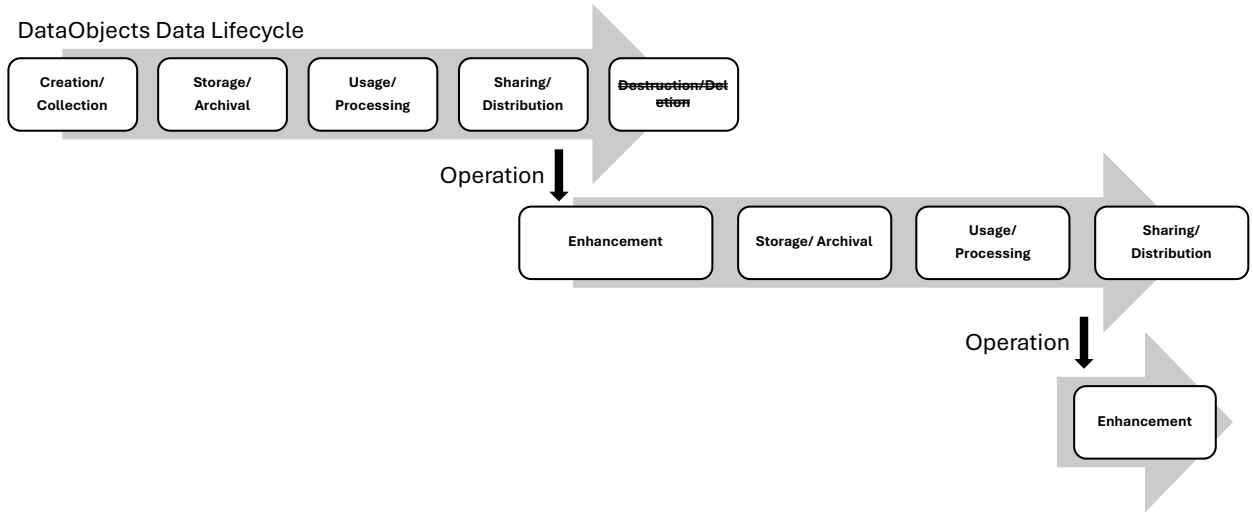
DataObjects seek to change the Data Lifecycle.

The traditional Data Lifecycle is shown below.

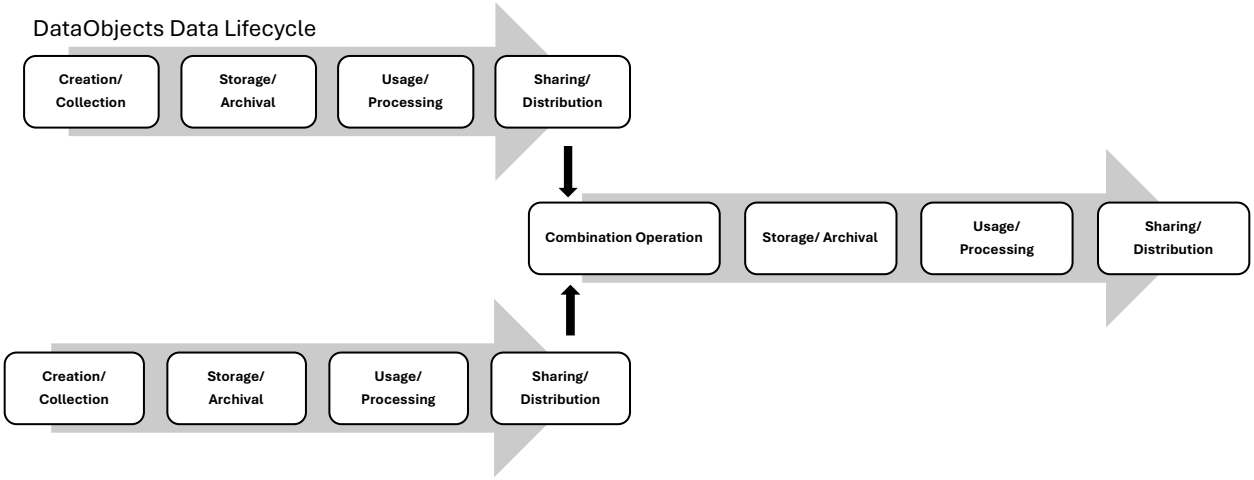


As DataObjects are immutable and are never deleted but become invalidated either through loss of confidence or being outside of their built-in validity conditions. Deletion is replaced by enriching data by transforming it via an operation and/or enhancing via a combination operation.

Serial Creation



Combining DataObjects



Benefits

1. Enhanced Data Security

By separating the validation process from data exposure, DataObjects drastically reduce the risk of data breaches. Data remains secure while still being verifiable, ensuring that sensitive information stays private.

Data can thus be stored on open storage networks, such as IPFS or DLT, as data exposure does not reveal ownership,

2. Interoperability Across Systems

DataObjects are designed to be interoperable across different platforms and systems. This means data ownership, history, and integrity can be tracked even as data moves between systems, networks, applications, and organizations.

3. Applications in Smart Contracts and Governance

DataObjects extend the smart contract model by adding verifiable ownership and privacy features. Smart contracts can now include terms that ensure data remains valid and confidential throughout the lifecycle of the agreement, allowing for more complex governance models and auditable systems.

4. Auditable Transactions

Every interaction with a DataObject is logged immutably, providing a secure and auditable trail of data usage. Further, with the help of an Identity Assurer, who manages the technical aspects of IDObjects, users can easily view all their data and its state. In the context of Digital Agreements, an auditor role in the agreement can be assigned that gives a trusted third-party access to the metadata of all data creation and usage ensuring it is being governed and used in line with the Agreement terms, without them having access to the underlying data the Digital Agreement creates or uses.

This is generally a good thing and particularly useful for compliance in sectors such as finance, healthcare, and government.

Conclusion

The **DataObject** is a transforming solution for data management that addresses the challenges of verifying data integrity, ownership, and confidentiality across systems. Its combination of cryptographic validation, immutability, and privacy-focused design opens new opportunities in sectors requiring secure, verifiable data exchanges. From digital identity management to complex smart contracts, the DataObject framework is ready to transform how data is managed and governed in the digital age.

By integrating **DataObjects** into data management systems, organizations can enhance security, streamline governance, and ensure the privacy of data, paving the way for a more trustable and secure digital ecosystem.

It is anticipated that the DataObjects, IDObjects, Digital Claims technology will be offered via license under the IDIO brand name soon.

Inventor: Ian Kelly; ian@idobjects.io

Patent Application: Computer Data Structure That Connects Data Claims Ownership and Agreements to Form a Congruent & Governed Data System

Filing Date: August 27, 2024