The SMART Protocol

Preamble

The financial industry is undergoing a profound transformation. As real-world asset performance data becomes essential to the transition economy, that economy will simultaneously gain unprecedented liquidity through the emergence of digital tokens. Asset tokenization offers the potential to unlock liquidity, streamline operations, and enable greater market access. Network protocols such as Canton play an important, but not the only role, in powering this transformation.

While Canton guarantees secure and consistent transaction processing, it is agnostic to the business logic driving those transactions. For instance, it can assure participants that a transaction is valid and private — but not that it reflects the correct business logic. That responsibility lies with the DAML smart contract, which encodes transactional logic and rights obligations. Yet even a smart contract is inherently self-contained; it does not possess awareness of the broader business application or context that led to its instantiation.

This division of responsibility is critical to understand. While the network protocol and the smart contract can successfully manage atomic business logic, it is not their functional role to understand distributed business applications, especially when that application requires the successful governance and coordination of many parties employing disparate business functions across a complex lifecycle of data spread over many smart contracts.

In short:

> *How can directly, indirectly, or tangentially connected entities ensure the broader system they interact through is governed with integrity and traceable provenance?*

This document outlines the principles, architecture, and use cases of the SMART Protocol, serving as the operational blueprint for building resilient, scalable, and tokenized information networks for the transition economy.

The SMART Protocol: Purpose and Analogy

Protocol Intent

The SMART Protocol is application, commodity, and token-agnostic. It is *not* a technical specification that addresses the specific mechanics of domains such as natural gas production or green bond issuance. Nor does it require the use of specific technologies like DAML or Canton—even though this document uses them for illustrative purposes. It does, however, require the underlying concepts of smart contracts and a form of token network protocol.

A Real-World Analogy: The Laptop Package

To make the protocol's principles more tangible, consider the following real-world analogy:

A laptop, which is a physical real-world asset belonging to an employer, is shipped to an employee in another country. This laptop has an asset identifier — let's call this the **Fiùtur SmartId**.

The sender packages the laptop and creates a shipping label. The package itself functions like a **tokenized smart contract**. It represents the rights and obligations related to transporting the laptop and acts as a governed construct with its own **Fiùtur SmartId** — in this case, the tracking number.

This tracking number uniquely identifies the package without revealing the underlying asset (the laptop) to unauthorized parties, making the process secure, transparent, and easily verifiable.

- It is self-contained, enclosing the laptop.
- It has signatories: the sender and the receiver.
- It involves a third party (the carrier), who plays a defined role.

Each party holds specific rights:

- The sender can initiate shipment.
- The receiver is authorized to open the package.

- The carrier may handle and transport the package but cannot open it or know its contents beyond a generic description.
- The carrier may use their own network to transport, but not necessarily a third party's.

All of this is governed by what's represented by the encoding on the label—no external "tokens" are needed by the sender or the receiver to achieve the task of sending the package from point A to point B.

Canton as the Carrier's Network Protocol

In this analogy, Canton represents the network protocol of the carrier. It defines how each node (e.g., depots, airports, trucks) must operate:

- Packages (i.e., smart contracts) are handled sequentially from node to node.
- Each transition is atomic, with rollback mechanisms in case of failure.
- "Track my package" status updates are tracked throughout the process.
- All movements must be traceable and preserve the privacy of the package contents

Expanding the Data Scope: Reference Data Set

Once the package arrives and the receiver signs for it, the carrier's task is complete. However, the receiver or the shipper may need additional contextual data for downstream needs (or applications), such as compliance, insurance, or sustainability. For example:

- Country of manufacture
- Warranty information
- Waybill and logistics details
- Scope 3 emissions data
- EU import certifications

This broader information set constitutes the Reference Data Set. While not present on the carrier's network or self-contained within the box (along with the laptop), it is vital for understanding provenance and enabling new applications. To the laptop owner, this data may be as valuable as the asset itself—especially for tasks such as risk mitigation, auditability, or regulatory reporting.

In short:

> *The SMART Protocol governs directly, indirectly, or tangentially connected data and entities to ensure the broader system interoperates with integrity and traceable provenance*

Expanding the Ownership Scope: The Physical Real-World Asset

As mentioned earlier, the laptop is a **physical real-world asset**, uniquely identified by its **SmartId**. Now, imagine that the employer (the original owner and shipper) decides to outsource all its IT operations and transfer ownership of the laptop to a third-party vendor.

Because the laptop has been tokenized and assigned a SmartId, the new owner gains several tangible benefits:

- **Tokenized Collateral**
  They hold a verifiable digital representation of the asset on a distributed ledger. This digital token contains key data about the asset's existence, provenance, and status.
- **Smart Contract Lock-Up**
  Both parties have agreed to lock the asset into a smart contract, which automatically enforces their business terms. This smart contract governs ownership rights and manages any claims, such as sustainability obligations (e.g., Scope 3 emissions reporting).
- **Reference Data Sets**
  The new owner gains transparent access to relevant reference data — for example, who received the laptop, which carriers transported it, and when. This creates an auditable chain of custody and provides insight into the asset's current performance status.
- **Liquidity & Efficiency**
  Tokenized collateral can be fractionalized, enabling innovative financial structures. For instance, the company could leverage its fleet of laptops and other physical assets as collateral to secure loans, improving capital efficiency and unlocking new liquidity opportunities.

Technical Scope

Digital Governance

Human and business processes, while important, are inherently fallible and often untraceable. Therefore, the scope of the protocol is strictly limited to calculations, validations, and smart contract operations that can be executed, verified, and traced within computer code. While external business processes and accreditations — such as SOC 2 — may serve as important inputs to the system, the protocol concerns itself only with elements that are digitally verifiable and digitally auditable.

System and Applications

In this document, the term “system” refers to a collection of applications operating concurrently. These applications, referred to as programs, each consist of interrelated and interdependent data entities, modeled as smart contracts. For example, a data KPI contract consumed by a bank may originate from multiple verified data source contracts, which themselves could be derived from a chain of other smart contracts representing readings, calculations, attestations, and verification processes.

Ecosystem Interoperability

Although applications operate independently, they exist within a shared ecosystem. Much like in natural ecosystems, they are distinct yet interdependent. For this reason, the SMART Protocol is enforced at a global level — no application may violate it without risking harm to the integrity of the entire system. By applying the protocol universally, interoperability is preserved, allowing consumers of tokens from different applications to compare, interpret, and trust data with a high degree of confidence.

Principles

Participants

All actors within the system must be identifiable and adhere to SMART Protocol's defined rules of engagement. While actors may assume different roles across various applications or programs — each potentially governed by distinct rules, such as conflict-of-interest policies or mandatory role assignments — the identity of an actor (or party) remains universal across the system. External processes, such as Know Your Data Provider (KYDP), can be employed to enhance trust, but the protocol itself remains agnostic to these processes and makes no assumptions about their implementation.

Participants:

- *Must be allocated a known and formal governance role within the system.*
- *Must be a party on the distributed ledger and their rights and privileges controlled at the smart contract level.*
- *Roles must be able to express mutual exclusivity to prevent inherent conflicts of interest between parties.*

Data Integrity & Quality:

It is not possible to represent all aspects of data and governance that led to a token's existence within a single digital token. As a result, the SMART Protocol recognizes that business data is best expressed through Reference Data Sets — collections of interrelated and contextualized data elements. Consequently, any data entering or generated by the system must conform to the relevant components of the SMART Protocol that uphold its quality, integrity, and coherence with its sibling data.

Data:

- *Must be governed by a physical location on Earth.*
- *May be temporally bound to production or measurement periods.*
- *Must be corroborated or verified by parties according to their governance roles without conflict of interest.*

- *Must follow a sequence of events that enforce the correct governance of roles and the correct application of data processes.*
- *Must adhere to formal digitally controlled restatement processes so any correction to data is justified and traceable.*
- *Must adhere to formal digitally controlled aggregation processes where assumptions and constants are persisted.*
- *Must offer formal data custody agreements so it is clear which entity has domain responsibility for the quality of the data.*
- *Must offer digital integrity of its lineage and interrelatedness.*

Datum Meaning and Interoperability

It is not enough to express the protocol of how data is managed and transferred, it is also important to manage data's meaning within the system.

Datum:

- *Must be known to a taxonomy or ontology to ensure its proper application within a larger set of datum.*
- *Must express its interoperability conditions as it relates to other sources or applications.*
- *When contributing to a common inter or intra-system concept datum must demonstrate its adherence to that concept.*

Token Lifecycle

Some tokens represent data with a defined lifecycle or a set of business rules governing their consumption. For example, a token representing a registered asset may progress through various stages: being registered, grouped into a pool with other tokens, encumbered by a separate business process, or ultimately consumed—after which it cannot be reused.

The SMART Protocol goes beyond isolated smart contract logic and focuses on the coordinated management of token lifecycles across the broader system. For instance, a token may not be eligible for encumbrance unless another token—representing a different but related concept—exists and is valid. This ensures lifecycle integrity and enforces dependencies across distinct data entities.

Asset Tokens:

- *Must reflect their current state, rights and privileges as distinct smart contracts.*
- *Must provide provenance and lineage to their entire lifecycle.*
- *Must demonstrate honoring their final consumption.*
- *Must provide lineage to their initial existence.*
- *Should offer a public or semi-public method of token existence check without needing to be party to the token.*

Summary

The SMART Protocol is an operational governance framework that enables the secure, scalable, and verifiable tokenization of real-world assets — from solar panels to large-scale facilities such as data centers and green ammonia process facilities. By defining how smart contracts, distributed ledgers, and reference data interoperate, SMART unlocks new liquidity and financing structures, turning traditionally illiquid assets into trusted, tradable collateral. This creates a significant opportunity for investors to participate in the transition economy's growth while ensuring that every asset's provenance, lifecycle, and sustainability claims are auditable and digitally enforced.

For investors, the SMART Protocol means higher confidence in asset-backed tokens and the networks that trade them. It does not tie participants to any specific technology stack but ensures that all transactions and data exchanges adhere to strict governance, conflict-of-interest safeguards, and cross-system interoperability. As industries increasingly tokenize their assets, SMART provides the blueprint for building resilient, trust-based markets that balance regulatory compliance with efficiency, enabling capital to flow into new asset classes with reduced operational risk.