HUMAN COLOSSUS FOUNDATION

The Human Colossus Trust Infrastructure Stack

Version 1.0

"Data" is at the core of the *Dynamic Data Economy* (DDE) as the kernel for transactional sovereignty and accurate exchange of information across a decentralised economic infrastructure. The volume of data generated by humans and machines continues to increase exponentially. Still, most data are either unused or their value exploited. Moreover, low trust in data-sharing, conflicting economic incentives, and technological obstacles have dampened the full potential of data-driven innovation. Therefore, it is crucial to unshackle the potential of data reuse by removing barriers across the data economy through open opportunities while fully respecting jurisdictional rules and human values. Furthermore, pivotal in the quest for innovation in the fields of analytics, artificial intelligence, or other data-driven applications, the potential for boosting a sustainable data economy by onboarding organisations into the DDE will ensure a more balanced collective mindset regarding the importance of data in line with the next wave of non-personal industrial data and the proliferation of Internet-of-Things (IoT) devices.

Regulating the flow and use of data while preserving high privacy, security, safety, and ethical standards is fundamental to grasping the digital age's opportunities in a data-agile economy.

Human Colossus Foundation (HCF)'s *Trust Infrastructure* stack presents *"Infrastructure"* versus *"Security"* incrementally through the core data domains as a tool to define and describe what contributes to creating a trust infrastructure for access and use of accurate data. Implementations that align with the stack will positively affect the relationship between DDE actors to incentivise cross-sectoral and jurisdictional data sharing.

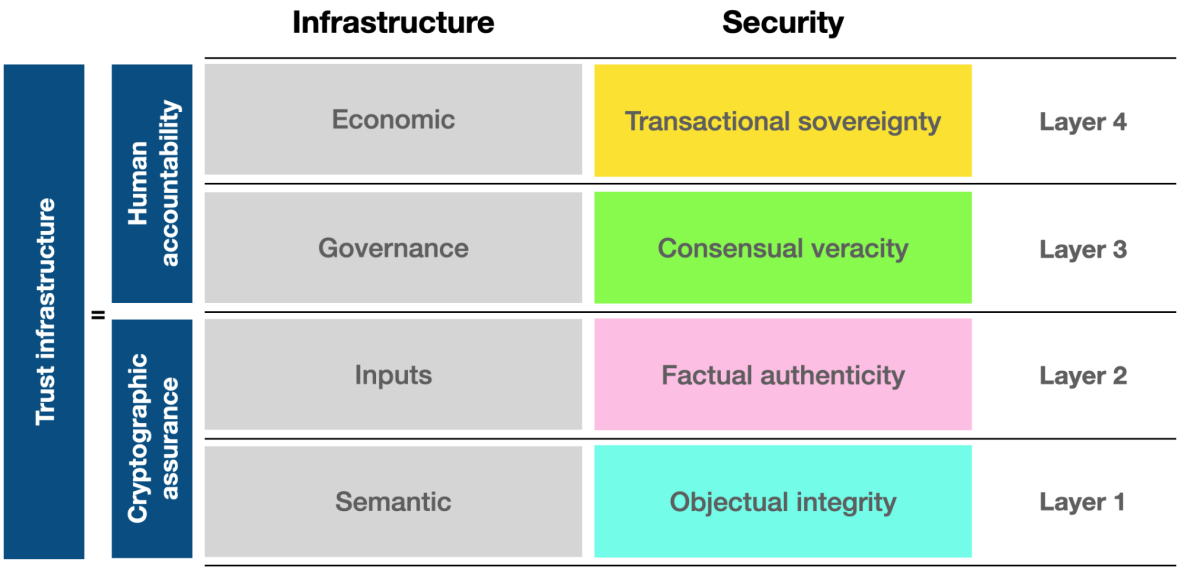

Figure 1. The Human Colossus Trust Infrastructure Stack

Sequential ordering starts with the *machine layers* (L1 and L2), supplying the cryptographic assurance to underpin the *human layers* (L3 and L4), where human accountability reigns. Collectively, these four layers constitute the *HCF Trust Infrastructure stack*.

Layer 1 (L1): Semantic infrastructure

"Integrity: the state of being whole and undivided"

A secure *semantic infrastructure* must offer ***objectual integrity*** through data capture, where semantic data models represent objects and their relationships deterministically to ensure the same results every time you run the model with the same initial conditions.

The four core DDE principles for the *Semantic domain* are:

- **Rich contextual metadata**: The captured context and meaning (the *"metadata"*) for all payloads MUST be rich enough to ensure complete comprehension by all interacting actors, regardless of written language.

- **Structured data forms**: Data governance administrations MUST publish structured data capture forms, specifications, and standards, driven by member consensus for a common purpose or goal that will ultimately benefit the global citizens and legal entities they serve.

- **Harmonised data payloads:** There are two areas of distinction to consider. Data harmonisation involves transforming datasets to fit together in a common structure. Semantic harmonisation ensures that the meaning and context of data remain uniformly understood by all interacting actors, regardless of how it was collected initially. Harmonised payloads are a MUST for multi-source observational data to ensure that the data is in a usable format for machine learning and Artificial Intelligence.

- **Deterministic object identifiers**: If the result and final state of any operation depend solely on the initial state and the operation's arguments, the object is deterministic. All object identifiers MUST be resolvable via the object's digest to be deemed deterministic.

Layer 2 (L2): Inputs infrastructure

"Authenticity: the quality of being real or genuine"

Underpinned by the semantic layer, a secure *inputs infrastructure* must offer ***factual authenticity*** through data entry, where signed timestamps accompany data inputs to identify the origin and creation of authentic events with the data considered factual.

Factual authenticity at L2 depends on substantiating the core security characteristic represented by L1.

The two core DDE principles for the *Inputs domain* are:

- **Authentic data events**: All recorded events MUST be associated with at least one public/private key pair to be considered authentic. Public/private key pairs provide the underpinning for all digital signatures, a mathematical scheme for certifying that event log entries are authentic.

- **Verifiable event identifiers**: Data provenance provides a historical record (an *"event log"*) of the data and its origins. All event identifiers MUST be cryptographically verifiable to ensure data provenance, which is necessary for addressing validation and debugging challenges.

Layer 3 (L3): Governance infrastructure

"Veracity: conformity with truth or fact"

Underpinned by the semantic and inputs layers, a self-regulating *governance infrastructure* must offer ***consensual veracity*** that the subjective nature of the rules for data access is epistemic to ensure the commitment of both the data controller and the intended recipient(s).

Consensual veracity at L3 depends on substantiating the core security characteristics represented by L1 and L2.

The five core DDE principles for the *Governance domain* are:

- **Reputable data actors**: Data governance administrations MUST exercise vigilance to ensure that all ecosystem participants involved in digital interactions under their administrative control are reliable and trustworthy.

- **Accountable data governance**: Data governance administrations MUST assume responsibility for the veracity of epistemic rules for safe and secure data sharing on behalf of the global citizens and legal entities they serve.

- **Searchable distributed databases**: Data governance administrations MUST house at least one distributed database that insights-based service providers can utilise for structured criteria searches and data requests.

- **Monitored data requests**: Data governance administrations MUST ensure that domain experts constantly monitor dynamic search engine targets under their administrative control to protect members against unethical or sensitive incoming data requests.

- **Consensual policy**: Privacy rights, data governance policy, and licences MUST provide the legal basis for safe and secure data sharing within and between sectoral or jurisdictional ecosystems for a particular purpose.

Layer 4 (L4): Economic infrastructure

"Sovereignty: supreme power or authority"

The security characteristics of the semantic, inputs, and governance layers form the foundational pillars to enable ***transactional sovereignty*** throughout a self-regulating *economic infrastructure*. Only then can safe and secure data sharing happen between engaged actors in any pairwise (peer-to-peer) exchange process or dyadic interaction.

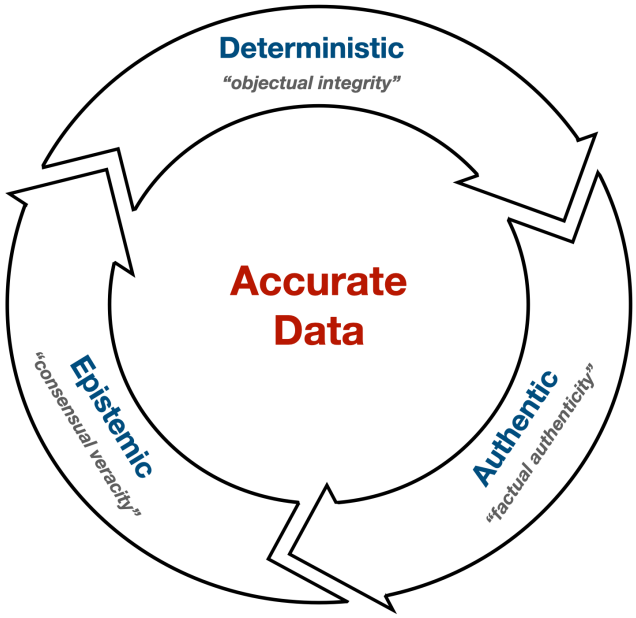

Figure 2. Core characteristic dependencies for data to be considered "accurate"

Transactional sovereignty at L4 depends on substantiating the core security characteristics represented by L1, L2, and L3.

The core DDE principle for the *Economic domain* is:

- **Encrypted data channels**: To avoid man-in-the-middle attacks, all digital transactions, bilateral agreements, and online communication between counterparties MUST be via secure, encrypted pairwise (peer-to-peer) communication channels.

The Human Colossus Trust Infrastructure Stack is a four-layer sequential stack that acts as a meta model to underpin any data-driven system or application. The four layers represent the foundational security design requirements of *objectual integrity* (Semantic domain), *factual authenticity* (Inputs domain), *consensual veracity* (Governance domain), and *transactional sovereignty* (Economic domain), thereby providing a robust framework to support safe and secure data-sharing ecosystem design considerations and, in doing so, the formation of a new Dynamic Data Economy - the DDE.