International Telecommunication Union (ITU-T) - **Study Group (SG 17)**

Focus Group - Metaverse (FG-MV)

The Metaverse – A New World of Asset Management, Security & Privacy

Edward Jerjian [CA]
Acquire Industries
CEO & Principal Engineer

11/04/2025

The Metaverse: Securing Physical and Digital Convergence

The Metaverse can be understood as a future **repository** of the real world and every interaction with it, but also a whole new world capable of infinite virtual possibilities – much like the Internet.

The Metaverse
Framework of virtual systems incorporating spatial referencing projected by technologies for interactive and meaningful experiences.

The challenge is securely linking RWAs to Digital Assets as their Digital Twin in the Metaverse, while maintaining **data integrity** and **user control**.

Real World Asset (RWA)
Tangible or intangible assets like real estate, goods, commodities, securities, intellectual property, and even individuals or aspects of the physical world (usually tokenized).

Digital Twin
Virtual representation of an object or system that is updated with real-time data throughout its lifecycle and helps with decision making through simulation, machine learning, and reasoning.

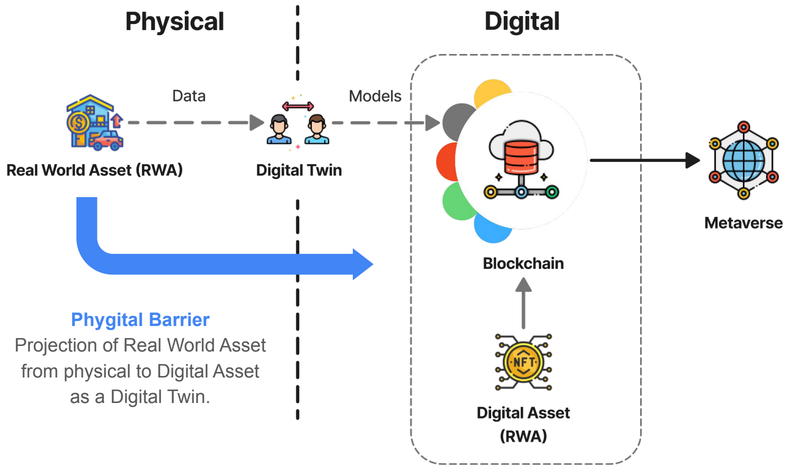


Diagram illustrating how a Digital Twin represents a RWA crossing the phygital barrier to become a digital asset which can be managed in the Metaverse.

ITU-T FGMV-20 Focus Group on Metaverse
ISO/IEC JSEG 15 Standards Evaluation Group - The Metaverse
ISO/IEC JTC1/SC41 (ISO/IEC DIS 24931-1)
Information Technology — Metaverse Part 1: Concepts, definitions & terminology

Digital Twins: Age of "Phygital" Media

Spaces

St. Peter's Basilica (Italferr) scanned using drones, georadar, airships and even laser topography to capture a 3D model and mappings to preserve information about the landmark as a "digital twin".

ITALFERR
GRUPPO FERROVIE DELLO STATO ITALIANE

Avatars

H&M

H&M creates 30 "digital replicas" of physical real-world models. Models own their "digital twin" and license their twin to other brands.

Objects

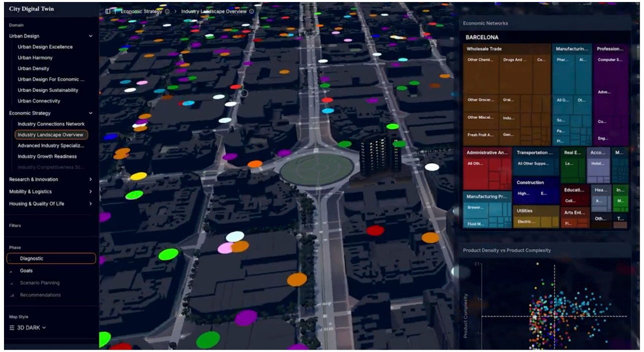
Courtyard.io

Courtyard.io provides custodial services, "minting" phygital copies of high-value collectible cards as NFTs to facilitate trading without leaving a secure real world vault.

Environments

City of Barcelona simulated digital twin based on domain level data like Urban Design, Economic Strategy, Mobility & Logistics, Housing and more.

ARETIAN
Urban Analytics and Design



The Metaverse as a Repository of "Phygital" Assets

Digital Twins may extend beyond passive models of people, artwork, collectables, buildings or entire cities. In the future, as technologies advance the Metaverse will be enabled as a repository for operating and analyzing RWAs as well as providing active experiences of phygital assets.

Classification of Digital Asset (RWA)

Classifications can be based on **fidelity** (low, medium, high) and level of **integration** with the physical world.

Level 1 - Passive

Observation. Primarily driven by historical or aggregated data, offering limited real-time insight. Security risks are lower but still present due to potential manipulation of the historical data.

Level 2 - Real-Time

Monitoring. Continuously receives live data streams from sensors and IoT devices attached to the RWA. This introduces significant attack vectors if the data stream is compromised.

Level 3 - Active

Control & Feedback. Receives data but also sends commands back to control the RWA (e.g., adjusting a person's body temperature or building heating based on occupancy). This represents the highest risk level due to direct interaction with the physical world.

Types of Digital Twins

Types can be based on **twinning rate** and **purpose** (operation, analysis, cloning).

Operational Twins

Used for operational data monitoring and control (e.g. sensor readings from a smart building's HVAC system). Security unauthorized access to control systems, with vulnerabilities impacting physical operations.

Analytical Twins

Used for predictive maintenance, simulations, and optimization (e.g., simulating the thermal profile of a building before construction). Data sensitivity increases, and breaches could lead to security and safety issues.

Identical Twins

Represent an individual avatar or asset within the Metaverse, incorporating biometric or sensor data, behavioral patterns, and interactions. This represents the highest level of sensitivity – misuse could have profound privacy and security consequences.

Active Identical Twin refers to both physical and digital aspects existing simultaneously in the real world and within the Metaverse.

Technology Gaps: Synchronicity between RWAs & Digital Twins

Crossing the **phygital barrier** is a matter of providing an interface to surveil data and patterns to be processed, which carries its own set of challenges. For that reason, Digital Twins of RWAs may be limited in scope based on the available **technology enablers** (e.g. AI) and not necessarily Metaverse-ready.

INTERFACE

Accuracy & Reliability: The quality of **sensors** used to capture data about the physical asset and **actuators** used to perform functions in the real world directly impacts the accuracy of the Digital Twin

Interoperability Standards: A lack of standardized protocols hinders seamless communication between different platforms and systems

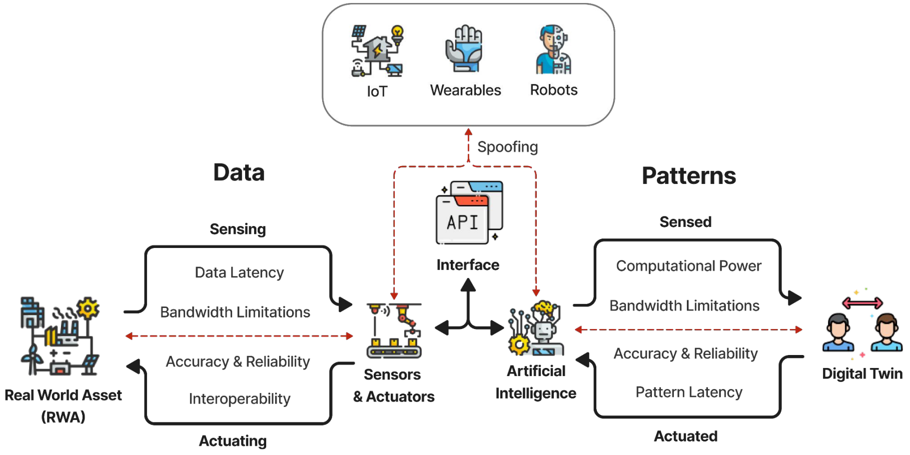
Spoofing: Malicious actors could inject false data into the RWA or Digital Twin, leading to incorrect decisions and potentially physical harm (e.g. manipulating a person's body temperature)

DATA PROCESSING

Data Latency: Delays in data transmission creates discrepancies between the RWA and its virtual representation, impacting decisions

Computational Power: Complex simulations and analyses within a Digital Twin require significant computational resources

Bandwidth Limitations: Streaming high-resolution **sensor** or **actuator** data can strain network infrastructure, creating vulnerabilities

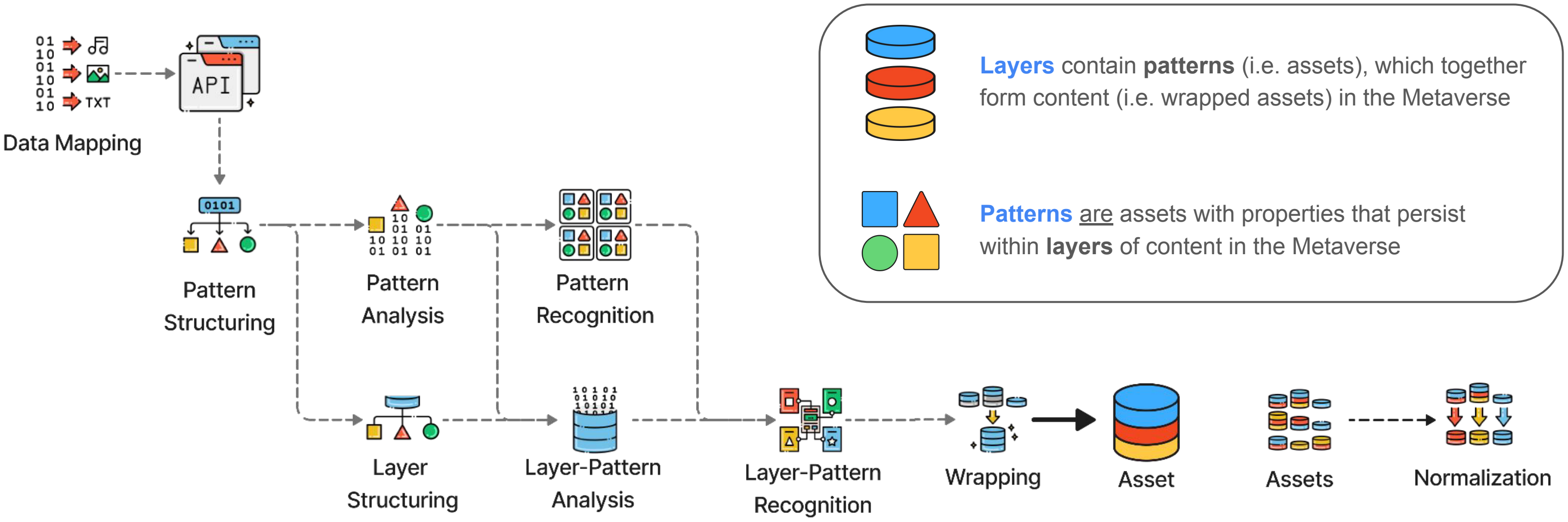


Data and pattern flow challenges in synchronizing a RWA with its Digital Twin – highlighting latency, limitations, inaccuracies, and the need for robust interfaces and security protocols.

In the Metaverse, we experience patterns not data.

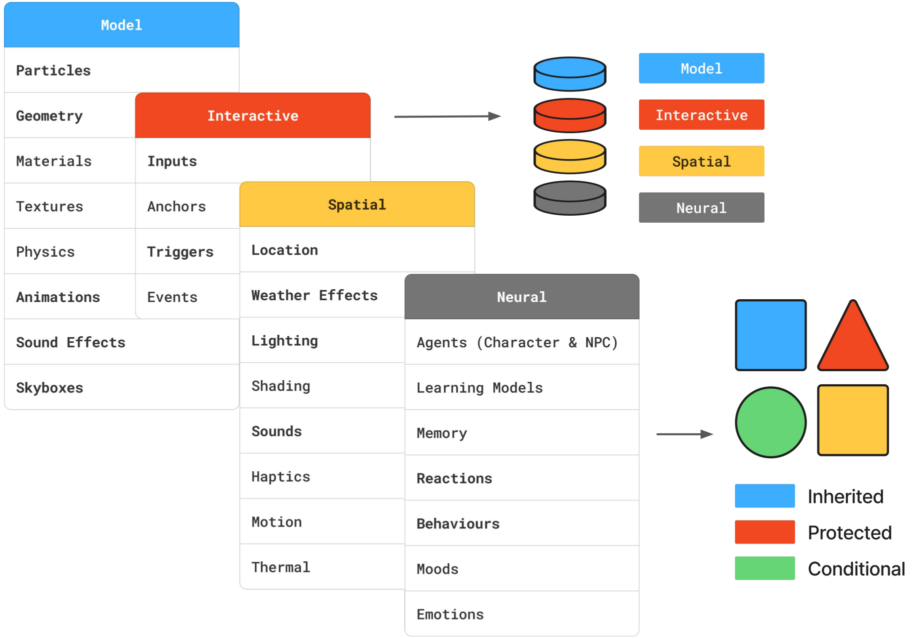
Metaverse Assets: Architecture Layers & Patterns

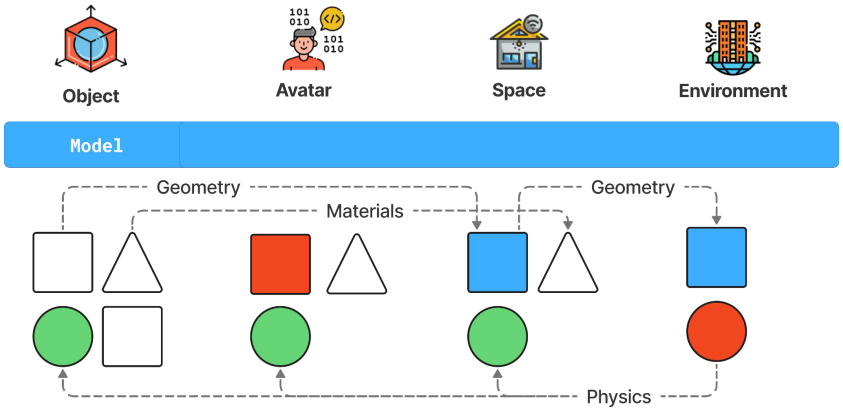
Using an informed approach from ISO/IEC/IEEE 42010 for reference architecture, we can separate concerns by **layer** in the Metaverse from the viewpoint of stakeholders in content creation. Metaverse assets are **patterns** (i.e. assets) working together to create **content** (i.e. wrapped assets).



Metaverse Assets: Architecture Layers & Patterns

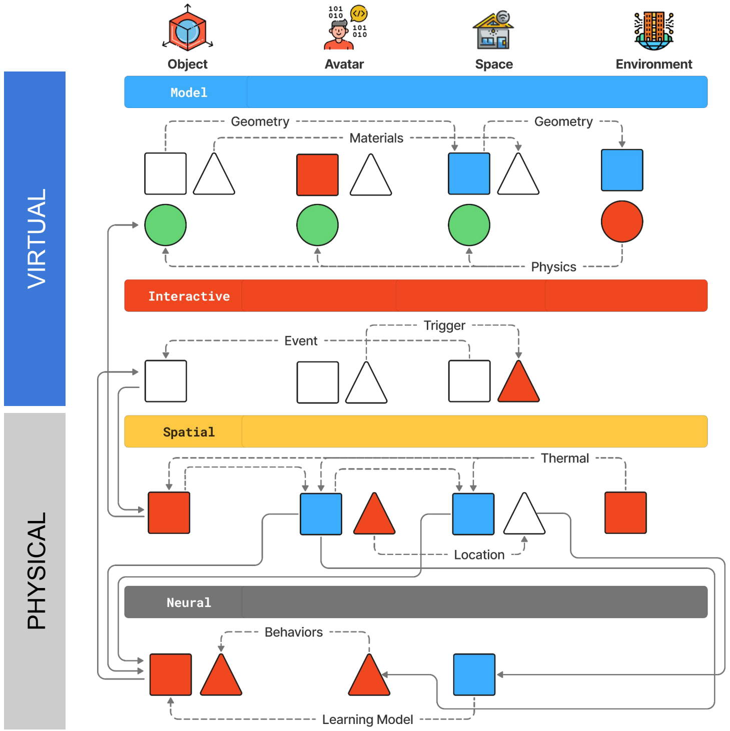
In the Metaverse, content types such as **objects**, **avatars**, **spaces**, and **environments** are comprised of patterns which persist across each layer. These patterns may include a **model** layer governing physical properties and **interactive** patterns of engagement and response to user input.





If it can be twinned, it's a pattern.

Metaverse Assets: Architecture Layers & Patterns



Stepping into the Metaverse, onto a heated floor in a shipping container.

Avatar (user) has geometry (i.e. body), skin, and physics
Object (floor) has materials with thermal properties
Space (container) has modeled boundaries and may be textured with insulation, or have other object components.
Environment includes physics and geometry, such as layouts of the components and objects.

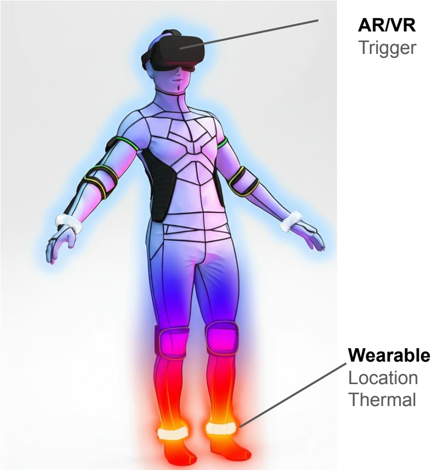
Avatar steps into a container, it triggers an event.
Space propagates an event pattern turning on the floor.
Object turns on and off, propagating thermal patterns.

Event initiates floor heating or modifies physics (like heat transfer increasing, or texture patterns with IR irradiance).

Object propagates thermal patterns to avatar and space.
Avatar movements through the space modifies spatial data patterns, experiencing heat both physically and virtually.
Environment creates a thermal context that may conditionally activate the heated floor (e.g. winter weather)

Avatar behaviours informed by thermal patterns of the body.
Space learns the location of the avatar which is inherited by the learning model of the Object.
Object turns on and off in areas based on location and behaviours.

This layer also can provide feedback loops from wearables (e.g. overheating causing behaviors).



Metaverse Assets: Stakeholders of Layers & Patterns

Stakeholder matrix reflects principles emphasizing the importance of clearly defining concerns and viewpoints in architectural descriptions to ensure systems are secure, interoperable, and contextually grounded in the governance, creation, interaction, and regulation of Metaverse Assets.

Stakeholder	Role	Responsibilities	Concerns	Actions
Owner	Integrity and security of RWA & Digital Twin	Data governance, access control, vulnerability, incident response	All layers (esp. Neural & Interactive)	Protects at all costs
Creator	Produces the twin and access interfaces	Data structures, security, management, exploits	Model & Interactive	Defines geometry, sets object physics (Model layer)
User	Interacts with RWA/Twin	Data privacy settings, consent management, awareness of risks	Interactive, Spatial	Triggers entry to a space, moves avatar (Interactive layer)
Platform	Infrastructure and services	Security audits, platform controls, authentication, data policies	Interactive, Spatial, Neural	Executes spatial simulations, manages thermal propagation
Processor	Processes RWA/Twin data & patterns	Data anonymization, encryption, compliance with relevant regulations	Spatial & Neural	Analyzes avatar behavior, triggers learning models (Neural)
Authority Having Jurisdiction	Regulations, codes, standards and enforcement	Data collection oversight, audits, enforcement actions	All layers (primarily Neural)	Sets max heating thresholds, requires reporting of unsafe behaviors

Metaverse Assets: Securing Access to Layers & Patterns

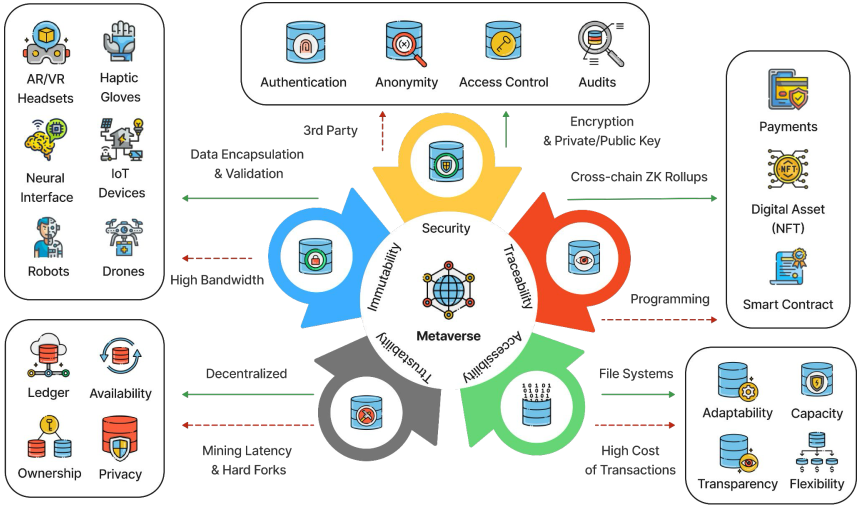
Key measures to be implemented would help mitigate the privacy leaks, eavesdropping, unauthorized access, phishing, data injection, authentication failures, and insecure design of the Metaverse.

Distributed Ledgers (DLTs): Blockchain technology provides an immutable record of transactions and access rights, enhancing transparency and accountability across patterns and layers.

Zero-Knowledge Rollups (ZKRs): ZKRs allow for secure computations without revealing the underlying data, protecting user privacy while enabling efficient transaction processing. They are particularly useful in scenarios like smart city infrastructure management and authentication.

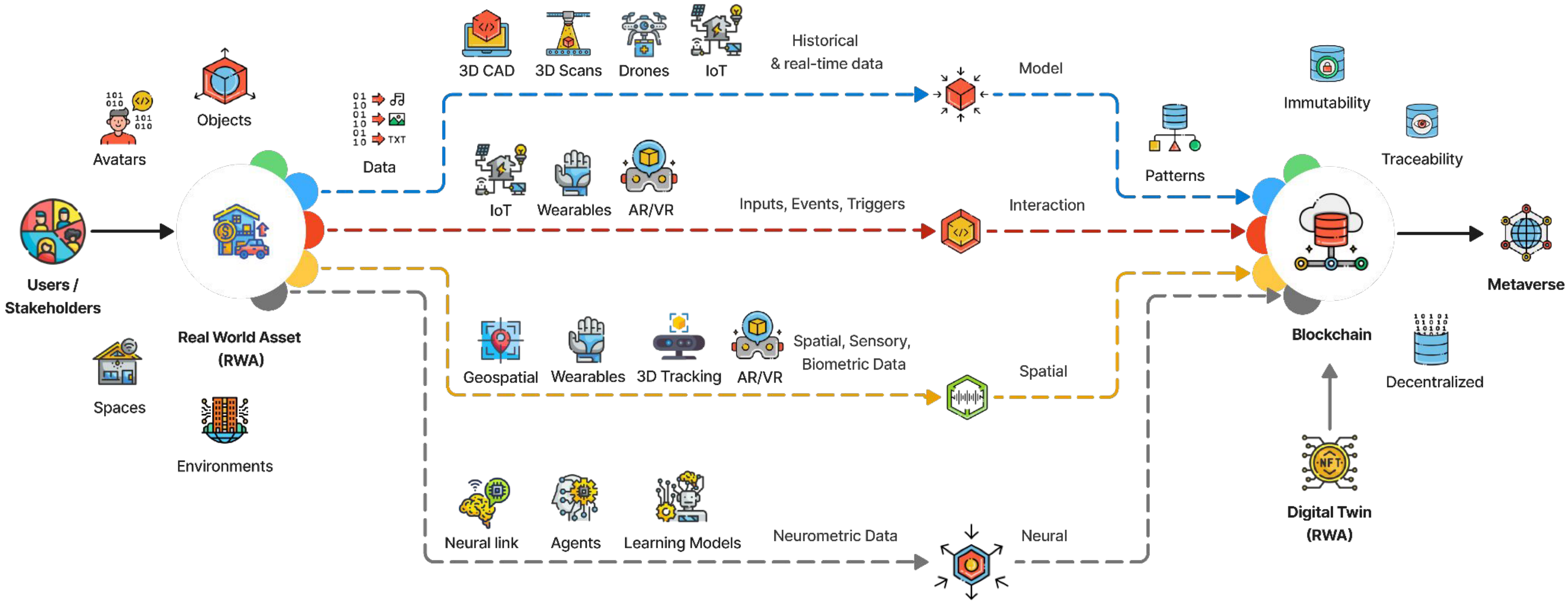
Homomorphic Encryption: This technique allows computations to be performed on encrypted data without decrypting it first, further safeguarding sensitive information.

Data Encapsulation: This techniques allows for data to be transmitted using ciphers (e.g. Vernam Cipher) from one device to another (i.e. data acquisition).



Blockchain supports the Metaverse with Security, Smart Contracts, Traceability, Immutability, and Decentralized infrastructure. Data Interoperability allows for assets, such as metaverse real estate.

Metaverse Assets: Layer Integration with Blockchains (DLTs)



The Metaverse: "Freedom to Operate" Approach

The framework should adapt flexibly to **regulations**, **codes**, and **standards** that align with specific needs and priorities, allowing for different levels of scrutiny based on risk profiles by **Authorities Having Jurisdiction (AHJs)**.

The Metaverse transcends geographical boundaries, creating challenges for determining which laws apply. A layered approach is needed.

Platform-Level Governance
Metaverse platform operators establish rules of conduct and enforce them through mechanisms like dispute resolution

Asset-Level Governance
Layers and patterns are regulated by creators and authorities. Smart contracts define the rights and responsibilities associated with specific digital assets.

Jurisdictional
Governments, regulatory authorities, certification agencies, enforcement bodies retain the right to intervene in cases of serious harm or illegal activity, potentially leveraging international cooperation agreements

Security & Privacy: Acts, Regulations & Standards

Data integrity and user control must be acknowledged and the inevitable diversity of regulatory landscapes.

- **GDPR (General Data Protection Regulation)**
  Focuses on data protection, principles of consent, and may need to adapt it by focusing on data minimization, purpose limitation, and user control.
- **IEEE/UL P2933**
  This standard for the clinical internet of things provides a valuable starting point but needs expansion to address security, privacy, and interoperability across the Metaverse.
- **EU AI Act**
  Regulation aiming to govern the development and use of artificial intelligence, including AI-powered access control systems.

The Metaverse is <u>not</u> extra-territorial.