The spectrum from database to registry

Verifiable credentials (drivers license, vaccine certificate, Aadhar card, …) are part of our daily lives. The W3C verifiable credential specification provides a mechanism to express these sorts of credentials on the Web in a way that is cryptographically secure, privacy respecting, and machine-verifiable. **Sunbird RC**, is a low code, no code open source project that uses a set of configurations to rapidly build out electronic registries of verifiable credentials - that facilitates enrolment, authentication, data ownership, search, issuance and management of verifiable credentials, claim attest flows between user and attester, sharing of credentials with DEPA compliant user consent, amongst others.

While, the Sunbird RC documentation provides detailed differences between database and registries, this document attempts to provide a set of concrete levels that span the spectrum between database to registries:

Level 1:
Structured data records in a database

Level 2: Standards/schema compliant (e.g. IDEA for agriculture), structured data records with unique id, accessible via API. Unique id should exist for the record itself and for each element of the entities referenced in the record e.g. land record having id for the land plot, id of the land owner, and id of previous ownership record),

Level 3:
Verifiable credential, that includes a digital signature of the attester/issuer in addition to features described in Level 2 in compliance with the W3C verifiable credential spec. In case of self attestation, the claimant and the attester is the user.

Level 4:
Attest-claim workflow that facilitates a claimant to get their self declared data (claim) attested by an attester and turned into an attested claim (verifiable credential).

Level 5:
Enrolment and authentication where the user can login and control their data. Note, if a user updates the data part of an attested claim (verifiable credential), then that record no longer remains a verifiable credential, it becomes a claim until again attested by an attester. At this level, revocation of a verifiable credential by the issuer should also be supported.

Level 6:
DEPA compliant consent management, ensuring no data gets used without user (data owner) consent.

Level 7:
Immutability, ensuring that no one can change verifiable credentials in the registry created in the past. This can be done by hashing and storing a registry record on a blockchain ledger or in a database with built-in cryptographic proof and verification e.g. Immudb. Here is a prototype of Sunbird-RC with CORD blockchain, and a prototype of Beckn with CORD.