Proof of Contribution Strategy for DLP Labs

DLP Lab's **Proof of Contribution Strategy** leverages the **DIMO API** to establish authentic permissions for accessing vehicle data, ensuring contributors have full control over what they share with DLP Labs. By using DIMO's "Login with DIMO" Oauth, we verify data authenticity, ownership, quality, and uniqueness while enabling a transparent and secure contribution process. Contributors are rewarded based on their permissioning level, which ranges from basic login to granting full permissions for valuable vehicle telemetry data. This approach empowers users to decide their level of participation while allowing for reward issuance based on the utility of the contributed data.

Reward Scoring System

1. **Baseline (25 Point):**
    - Action: Contributor logs-in via the DIMO API.
    - Validation: Event log `LoginVerified` confirms authentication.
    - Data: Dimo Wallet Address is captured, which is different from the EVM address
2. **Partial Contribution (25 Points):**
    - Action: Contributor provides verified vehicle make and model.
    - Validation: Event log `VehicleRegistered` confirms data submission.
    - Data: Collect a Dimo Wallet Address along with Make/Model of the vehicle attachesed
3. **Full Contribution (50 Points):**
    - Action: Contributor grants full permissions for telemetry data.
    - Validation: Event log `PermissionGranted` confirms scope of permissions.
    - Data: All vehicle data is accessible by Auto DLP including VIN specific details.

Workflow Example

1. **Contributor Action:** User logs into DIMO, registers their vehicle, and grants permissions.
2. **Event Logs:**
    - `LoginVerified`: Confirms authentication.
    - `VehicleRegistered`: Confirms vehicle make and model submission.
    - `PermissionGranted`: Confirms full permissions for data use.
3. **Data Hashing:** Vehicle and telemetry data are hashed and stored on-chain by Dimo
4. **Prover Process:** Prover fetches the vehicles associated with the connected account and attempts to fetch telemetry data.

5. **Reward Distribution:** Contributors earn rewards based on their permission level. We grant rewards to users who submit permissions for us to utilize the contributions

---

1. Authenticity

Objective: Ensure the data submitted is authentic and untampered.

Method:

- Contributions are logged through the DIMO API, which generates authenticated event logs upon user actions (e.g., login, vehicle data submission, permission grant).
- Vehicle make and model data are validated against DIMO's datasets.

Tools/Processes:

- **DIMO API:** Provides real-time validation of user identity and vehicle data, which is a wrapper for fetching on chain data.
- **Hash Storage:** Vehicle data submissions are hashed and stored on the Dimo network for immutability.

Validation:

- OAuth with Dimo guarantees authenticity against the Dimo data which we validate as part of the proof generation

---

2. Ownership

Objective: Confirm that the data contributor owns the data they submit.

Method:

- Contributors authenticate through the DIMO API, linking their account or wallet to the vehicle data.
- Ownership is validated by verifying the vehicle make and model against records accessible via DIMO's platform.

Tools/Processes:

- **DIMO Ownership Verification:** Confirms ownership through authenticated vehicle registration data.
- **Consent Records:** Immutable consent metadata stored on-chain verifies user permission for data use.

Validation:

- Validators confirm that the wallet address in the `PermissionGranted` event matches the user's identity and the grantee is the Auto-DLP client
- Metadata is cross-referenced with DIMO's ownership database to ensure alignment.

---

3. Quality

Objective: Ensure the data submitted is complete, accurate, and valuable.

Method:

- Data completeness is verified by ensuring all required fields (login, vehicle make and model, permissions) are provided.
- Vehicle data is cross-checked against known patterns to eliminate errors or inconsistencies.

Tools/Processes:

- **DIMO API Completeness Check:** Validates that vehicle information (make, model, year) matches required fields.
- **Telemetry Data Validation:** Optional telemetry data is validated for consistency and accuracy if full permissions are granted.
- **Contributor Feedback:** Users are notified to correct incomplete or inaccurate submissions.

Validation:

- Validators perform spot checks on submitted data to ensure accuracy.
- Validators perform a token exchange to get granular information on data shared

---

4. Uniqueness

Objective: Ensure the data submitted is unique and not duplicated.

Method:

- A unique ID is assigned for each dimo wallet collected and tracked within our services.
- Dimo assigns a unique `ContributionID` for each data submission tied to the wallet and vehicle information.

Tools/Processes:

- **Deduplication Algorithm:** Flags duplicate submissions by comparing on-chain hashes.
- **Unique Contribution Tracking:** Relying on Dimo for de-duplication which uses logs metadata (e.g., `ContributionID`, timestamp)

Validation:

- Currently each dimo wallet, which is different from the EVM wallet) can only have one file published. The published file will be scored.
- Duplicate contributions are not proven, and skipped.
