SELF SOVEREIGN IDENTITY

A BLOCKCHAIN USE CASE

DISCLAIMER

The opinions presented/stated during this workshop are of the speakers alone.

They are not to be attributed to anyone else.

AGENDA

- What is identity
- Centralized Identity Solutions
- Federated Identity
- Self Sovereign Identity
- Why Blockchain

WHAT IS IDENTITY

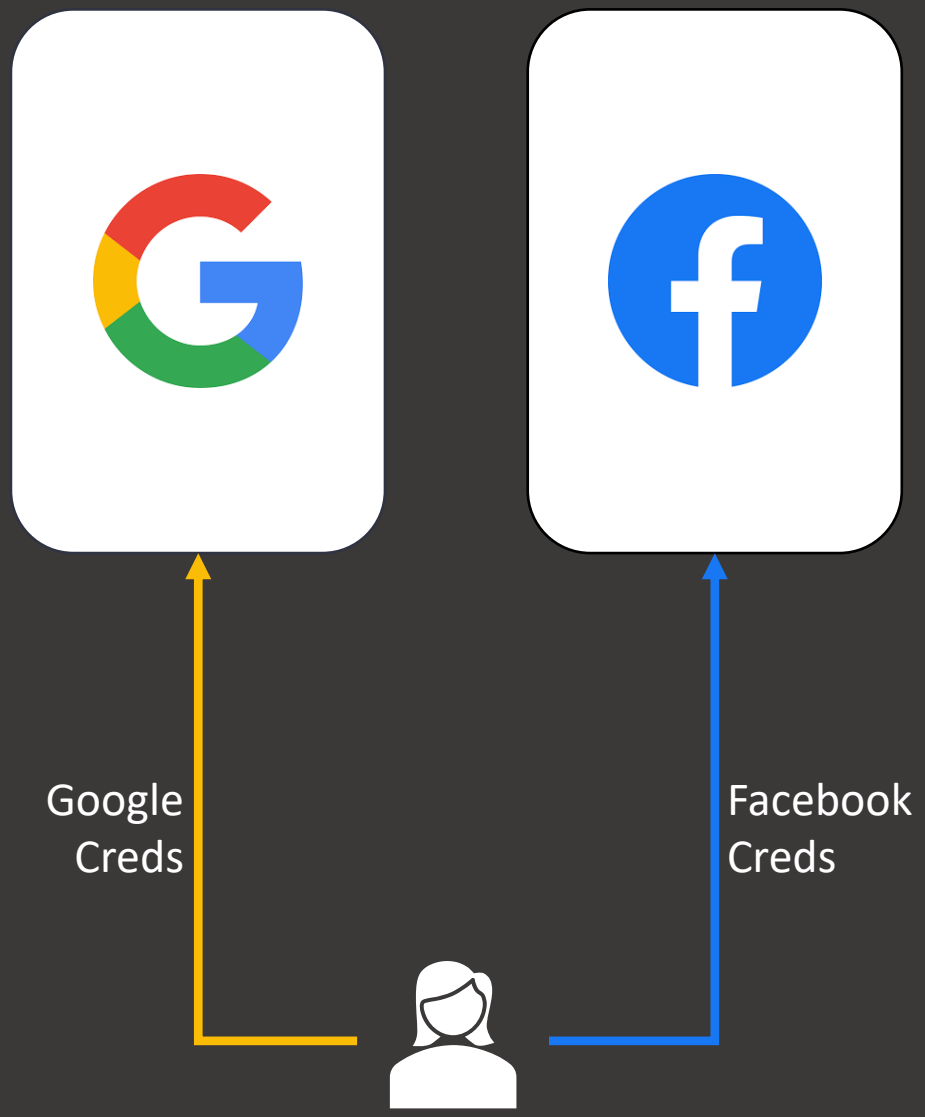
Who am I?

- Any data that can be used to identify, interact with or classify an entity forms a part of its identity
- Two types of identity fields
  - Self evident
  - Endorsed
- Trust on endorsed fields is dependent on the endorser

DIGITAL IDENTITY

Who you are?

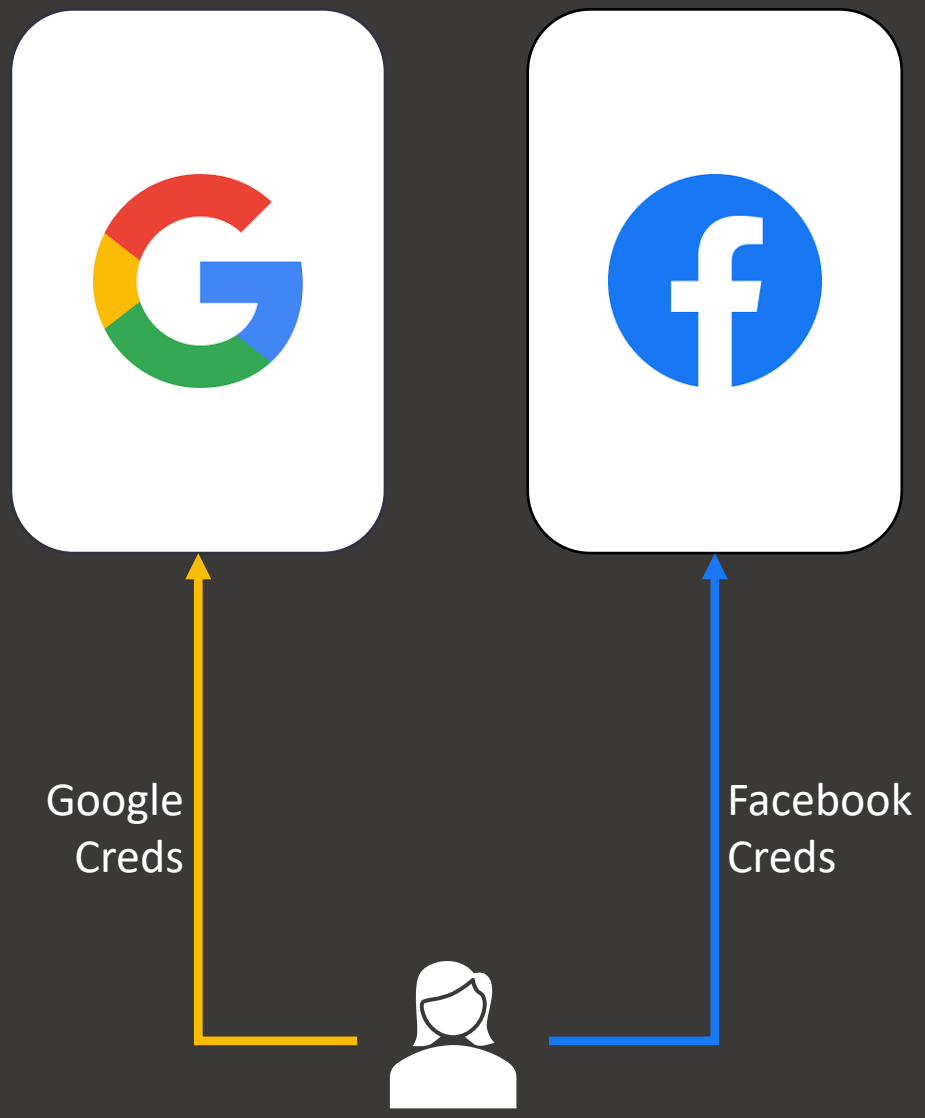
- Online services need to identify user
  - Across interactions
  - Across different products
- This needs assignment of a unique identifier to the user for identification
- Also there needs to be a mechanism to ensure exclusive access through this identifier
- Some services may need references to additional identity data



CENTRALIZED IDENTITY

To each its own

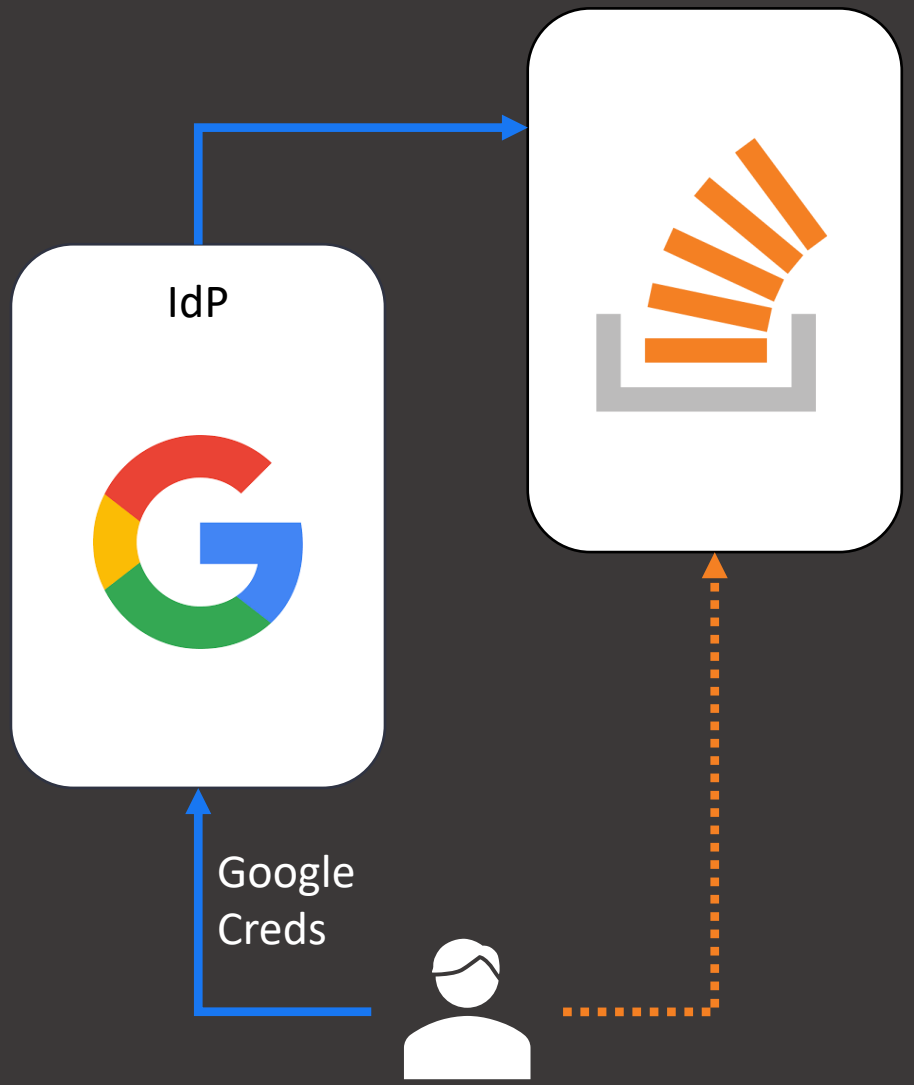
- Each service provider maintains own identity registry
- User has to create an account using the onboarding process set by the service provider
- Account with one service provider cannot be used in any form by another service provider



CENTRALIZED IDENTITY

What are the issues?

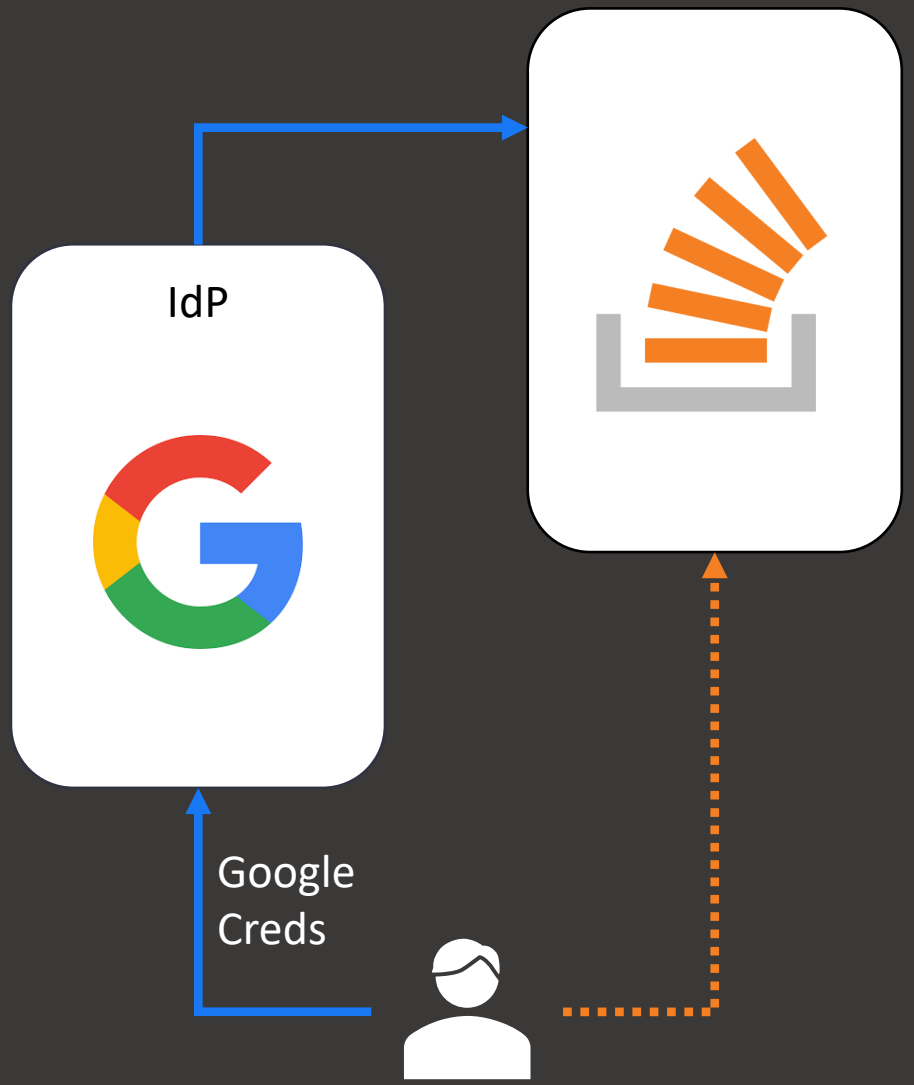
- User has to manage a large number of credentials
- Onboarding process has to be repeated for each service
- Each system with personally identifiable information becomes a target for attack
- Users have no control over how the data is being used by the collector or shared with 3rd parties



FEDERATED IDENTITY

Reusing user identity

- Identity providers (IdP) provide user identification services
- Service providers can outsource the critical auth functionality to specialized players
- This allows reuse of accounts thus reducing password fatigue
- Onboarding process is smoother



FEDERATED IDENTITY

What are the issues?

- The IdP becomes a single point of failure that may affect access to multiple services
- IdP can profile user interactions across services leading to privacy concerns
- 3rd parties can corelate data across services using a common identifier to create a user profile
- The user still has no control over the data collected

WHAT DO WE NEED?

Reinventing identity on the web

- User must be the owner of her identity
- User must have control over her data
- An entity should be able to endorse claims for a user
- Another entity should be able to independently verify such endorsements by other parties
- It should discourage profiling through triangulation of data from multiple sources

DO WE HAVE SUCH A SYSTEM?

SELF SOVEREIGN IDENTITY

USER

- Create an identifier for self
- Share the identifier with a proof of ownership
- Receive and hold claim endorsements
- Share claim endorsement data or proof of compliance to a constraint with a requester

ISSUER

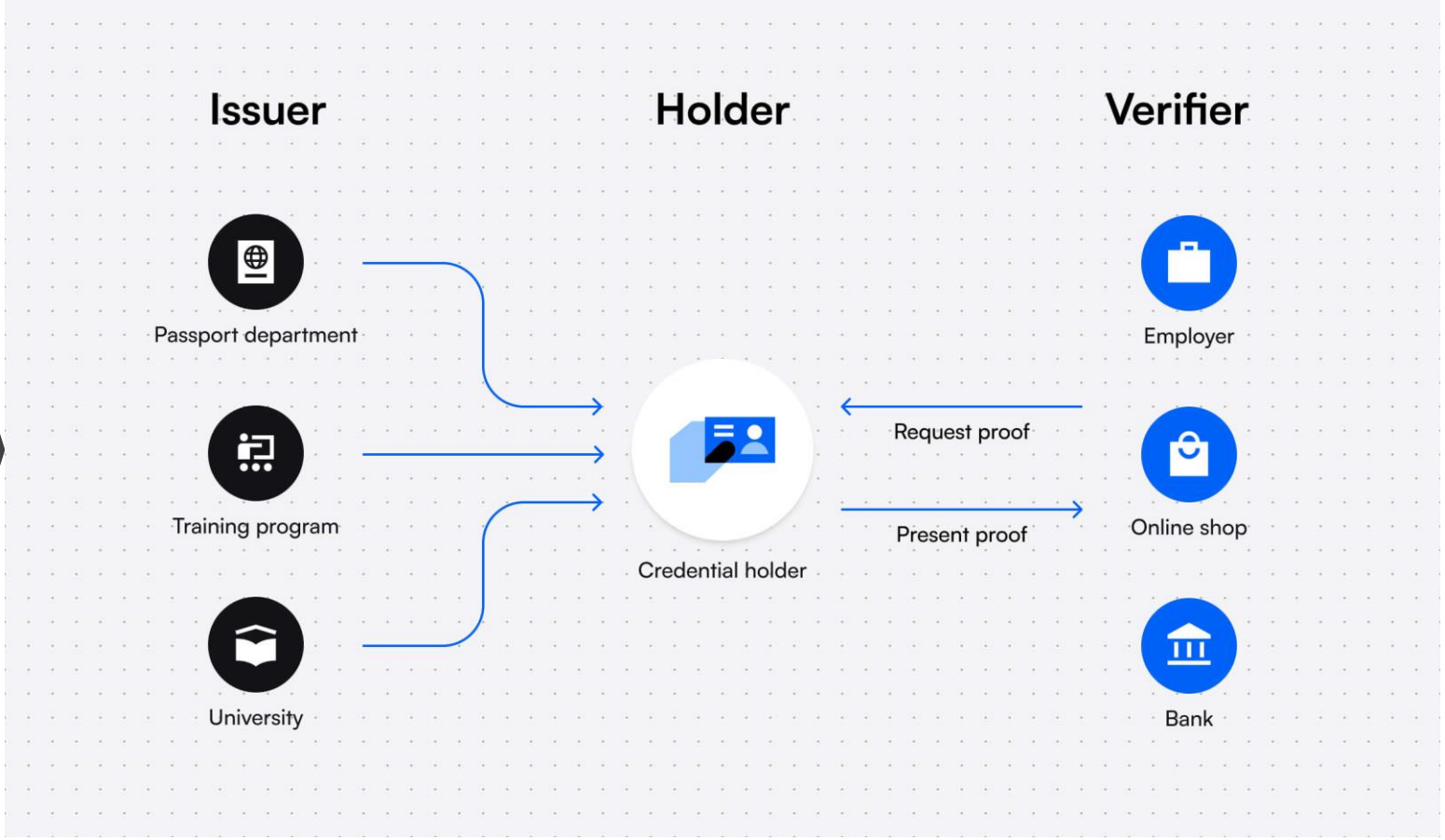
- Accept requests for endorsements
- Verify ID and proof attached to the request
- After required checks, create a verifiable claim with details of aspects about the identity being endorsed
- Share the verifiable claim with requester

VERIFIER

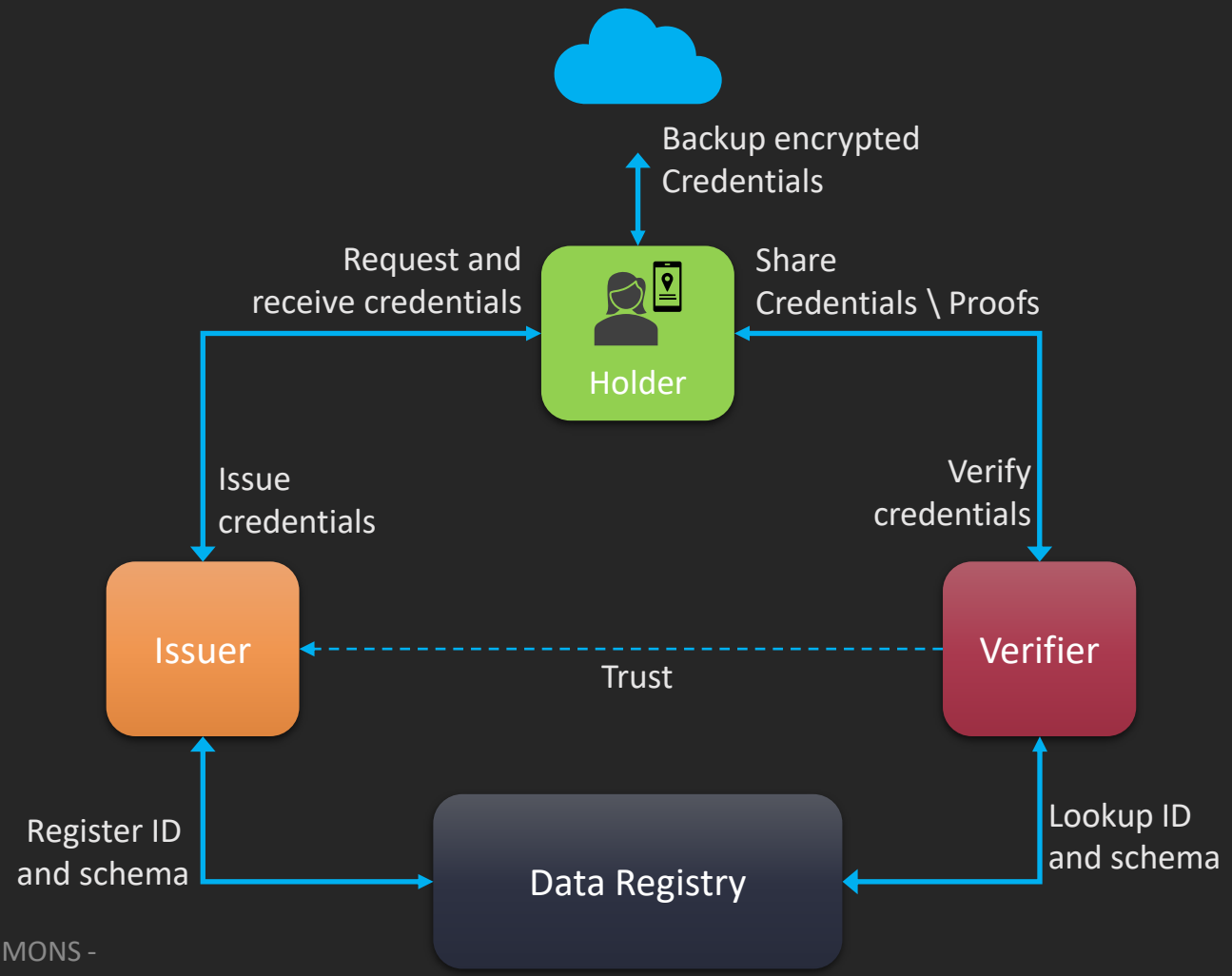
- Request the user to share specific data
- Accept response from the user
- Verify the claims and associated proofs without any interaction with the issuer

DO WE HAVE SUCH A SYSTEM?

EXAMPLE SSI SCENARIOS



SSI ARCHITECTURE



THE DATA REGISTRY

Why do we need it?

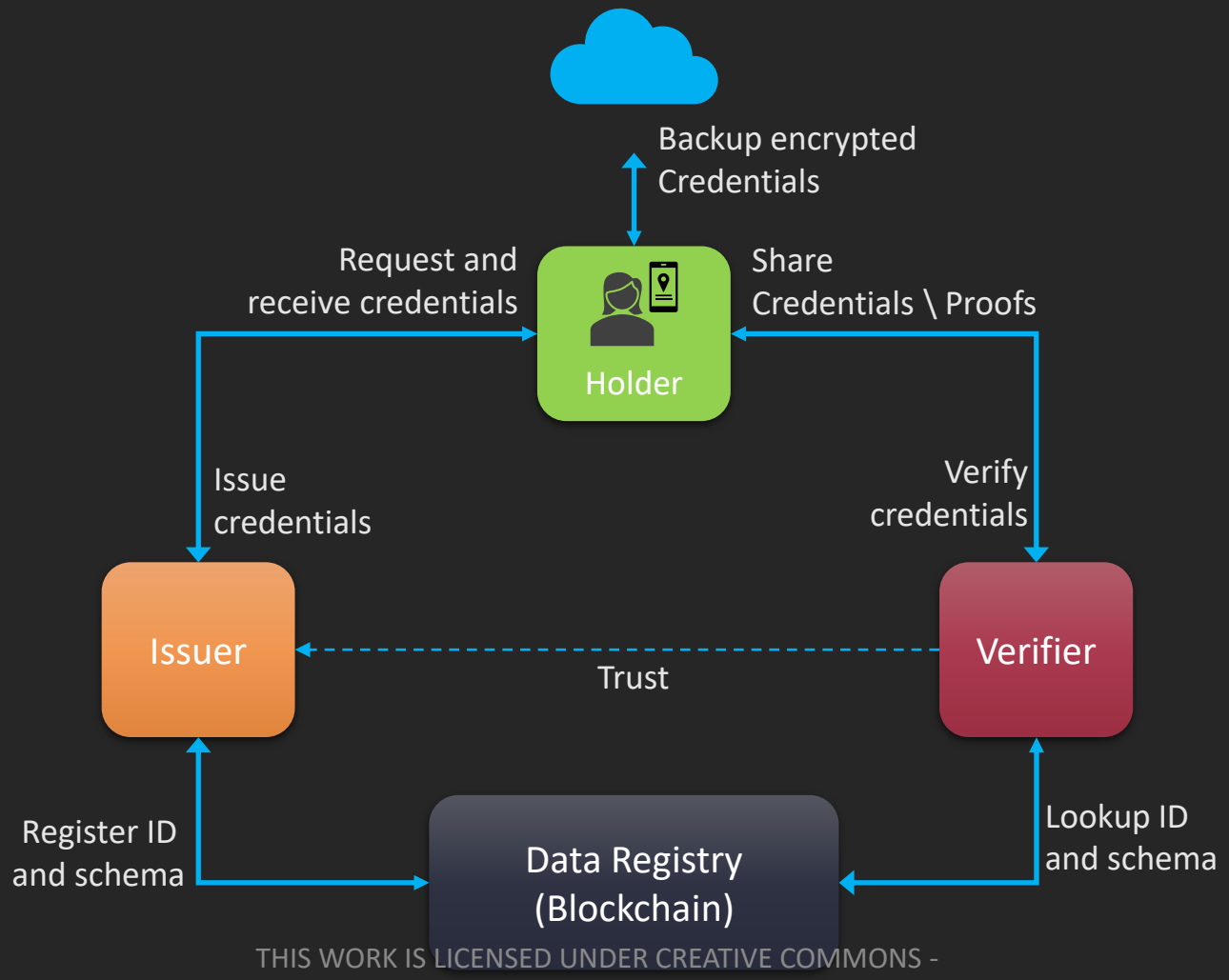
- The issuer should be able to publish
  - Its Identifier
  - Structure of the credentials being endorsed
  - Other metadata
- The verifier should be able to fetch any issuer related data needed for credential verification, without any involvement from issuer

THE DATA REGISTRY

Desired qualities

- Must not be controlled by the issuer
- Should not be single point of failure
- Should be open for read & write enabling interoperability
- Should be tamper proof
- Should support custom logic to govern the data being stored

SSI ARCHITECTURE



DEMO

https://www.youtube.com/watch?v=kcuJCOTaS8s

THANK YOU