PII Data Privacy Solution

Armin Moridi

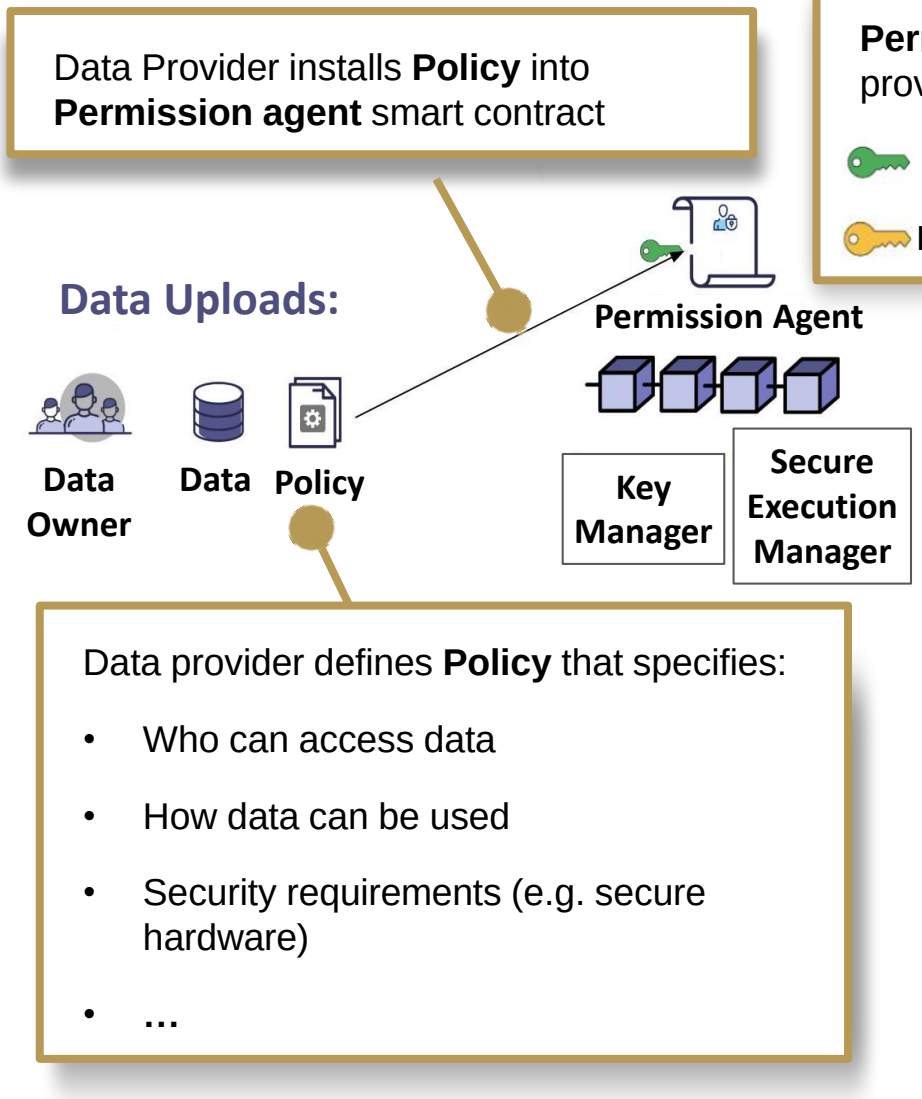
U.S. Patent Application 16/846,081
Title: Systems and Methods for data Privacy and Security K&B Ref.:
51778-20003.00

How do we ensure security and confidentiality at rest?

To ensure data security at rest, **Data Providers define policies around data encryption/usage and provision two keys** - a public key used to encrypt and verify data, and a private key used to decrypt data held by a key manager.

- **Public Key:** Shared with the data provider to encrypt data entering the system.
- **Private Key**: Held by the secure key manager and used for data decryption. It can only be accessed by the permission agent
- **Key Manager**: Holds private keys. It is decentralized to ensure no single point of failure

  - Keys are split across various key managers
  - Ensures keys are not leaked even if a single key manager becomes compromised



Compatible with current security systems

↓

Not much effort to modify the system

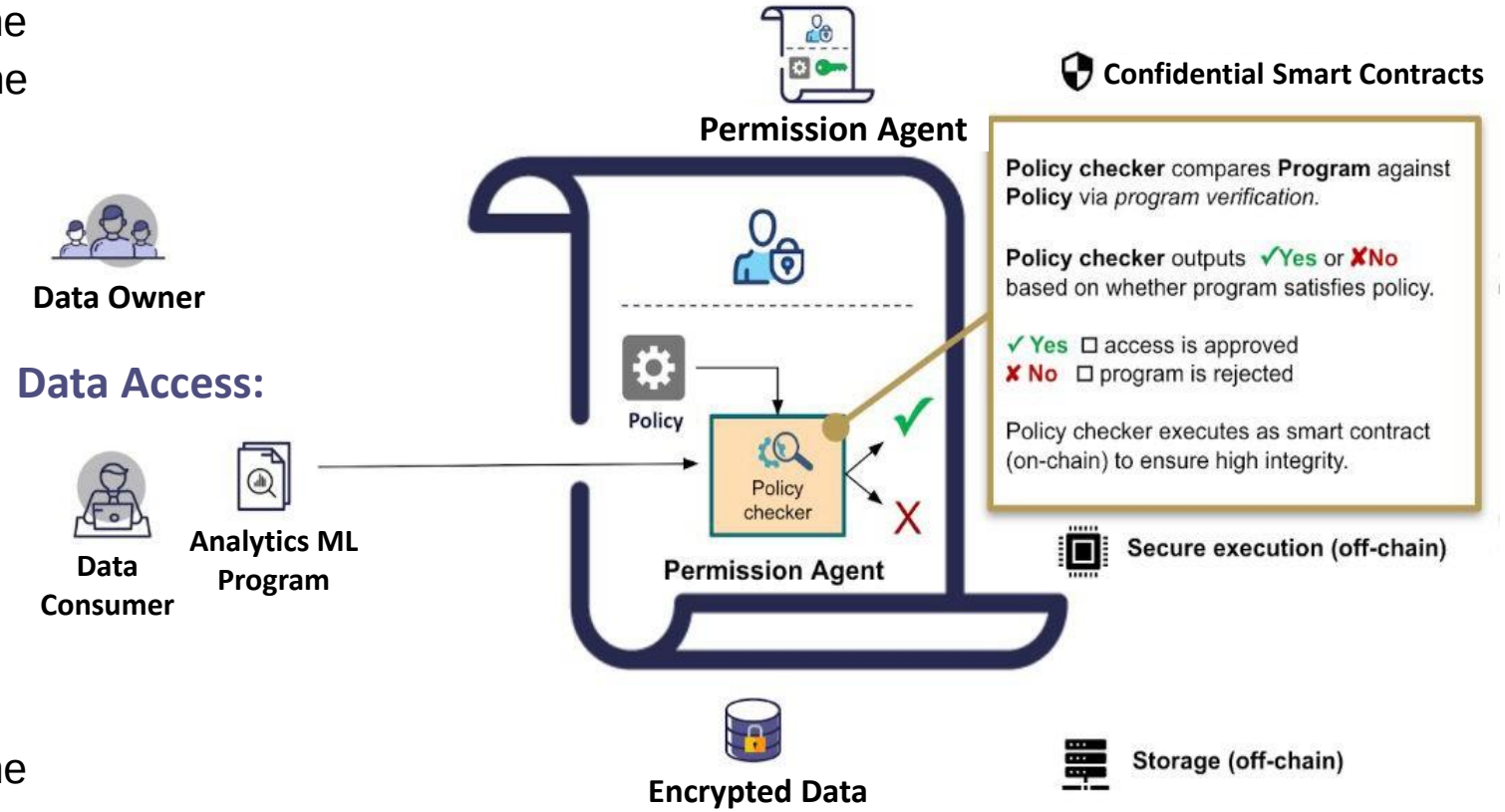
What about Data in use?

When the Data Consumer submits a program, the permission agent checks the program against the data provider's data policies to verify access.

If access is allowed (i.e. the policy is satisfied):

1) The request is logged on a distributed ledger to provide an immutable record of actions
2) It triggers the launch of a secure execution environment (typically a secure enclave) and the specific data needed is loaded into the enclave.

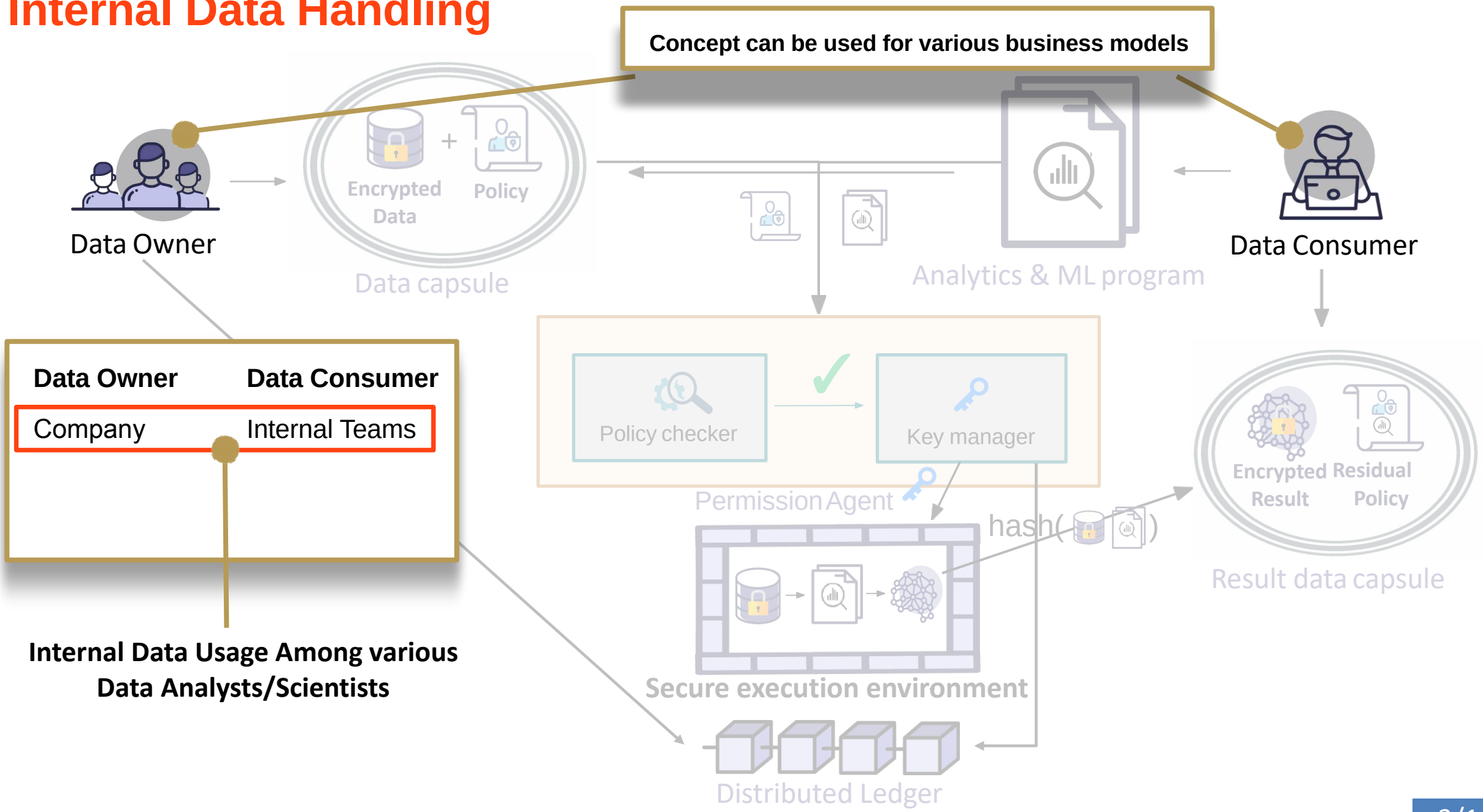
The specific data is then decrypted only *inside* the enclave, where the action requested by the Data Consumer also runs



Decrypted data never leaves the secure enclave

In the next 10 slides "Data in Use" methodology is explained

Internal Data Handling



External Data Handling

Concept can be used for various business models

Data Owner

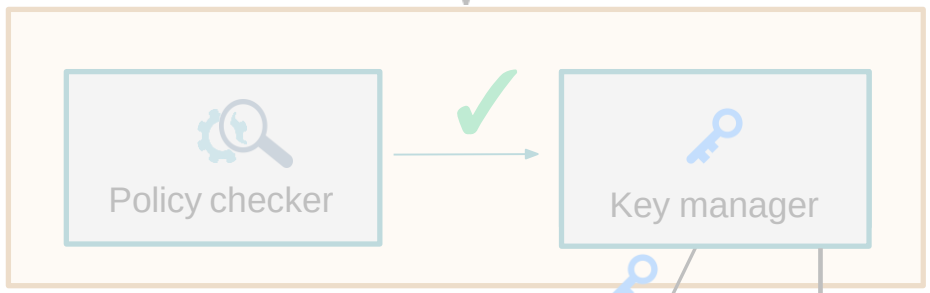
Data capsule

Analytics & ML program

Data Consumer

Data Owner	Data Consumer
Company	Internal Teams
Company	Third Parties

Full Control on how an external party will use the data



Secure execution environment

hash( )

Result data capsule

Distributed Ledger

User Consent Management

Concept can be used for various business models

Data Owner

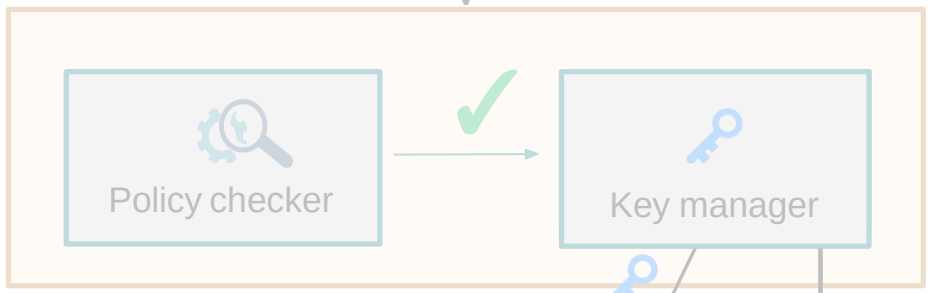
Data capsule

Analytics & ML program

Data Consumer

Data Owner	Data Consumer
Company	Internal Teams
Company	Third Parties
User	Company

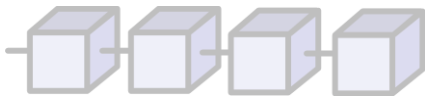
Users can take control of their Data Compliance with Privacy Laws (CCPA and GDPR)



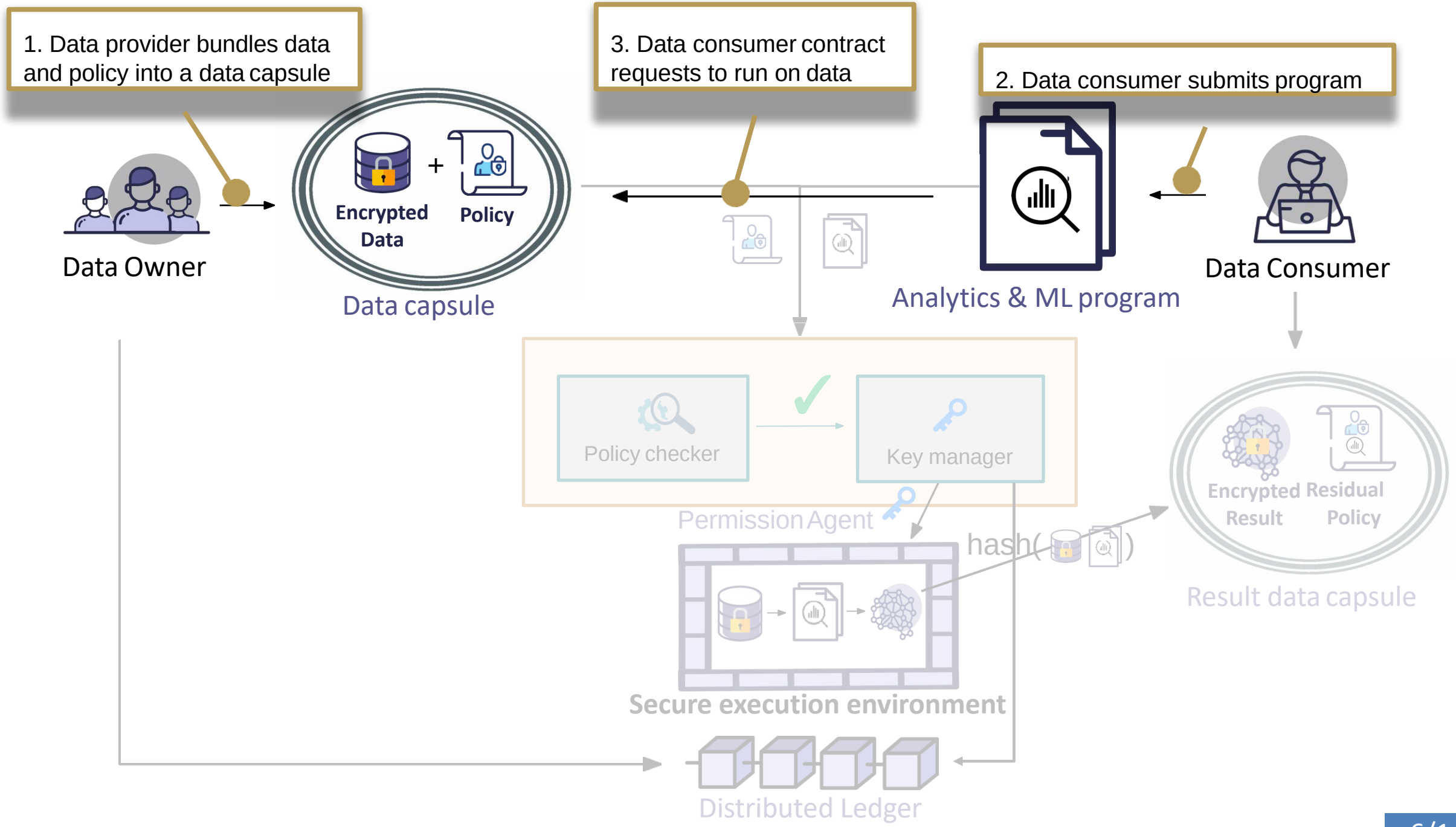
Secure execution environment

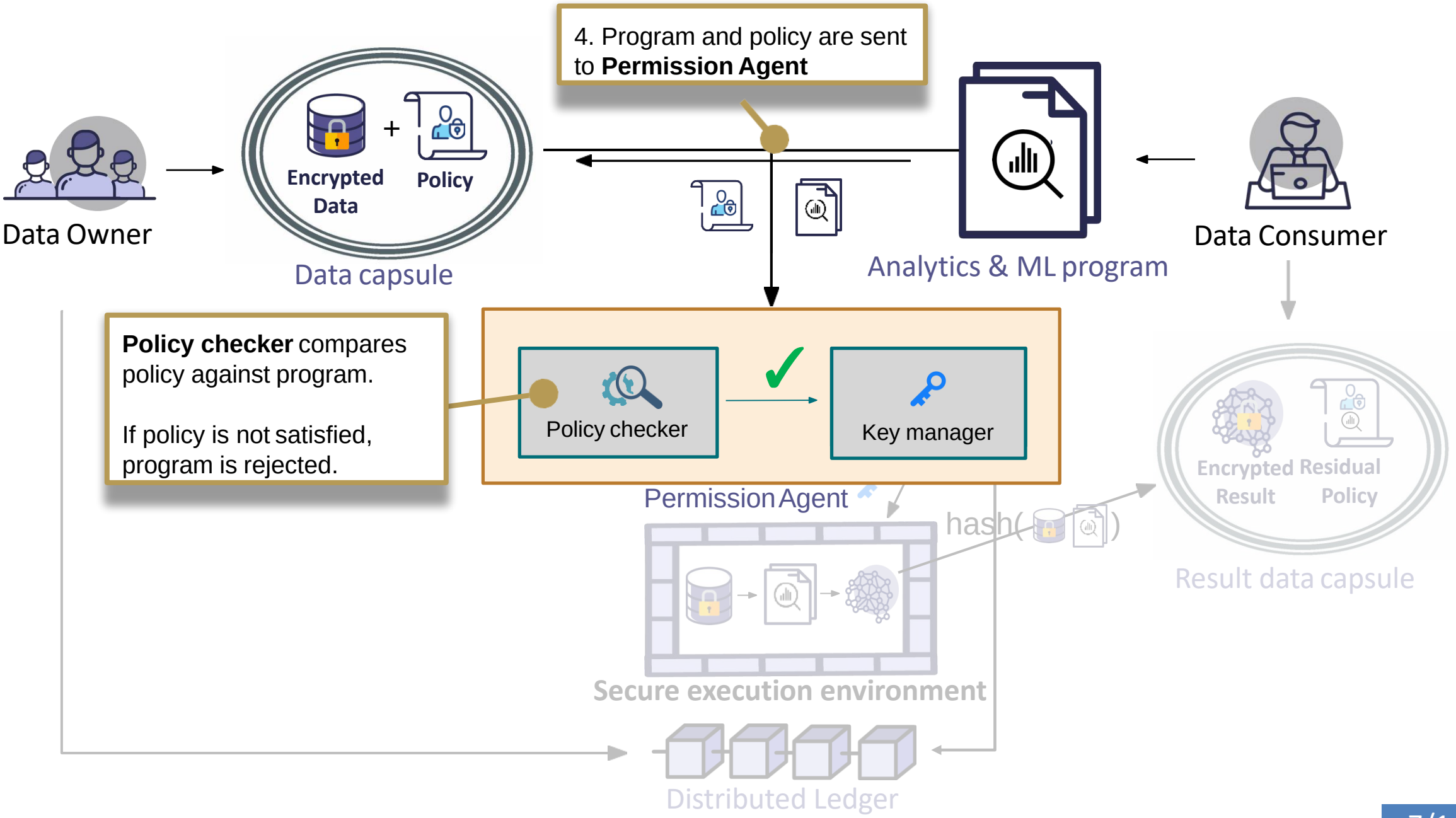
hash( )

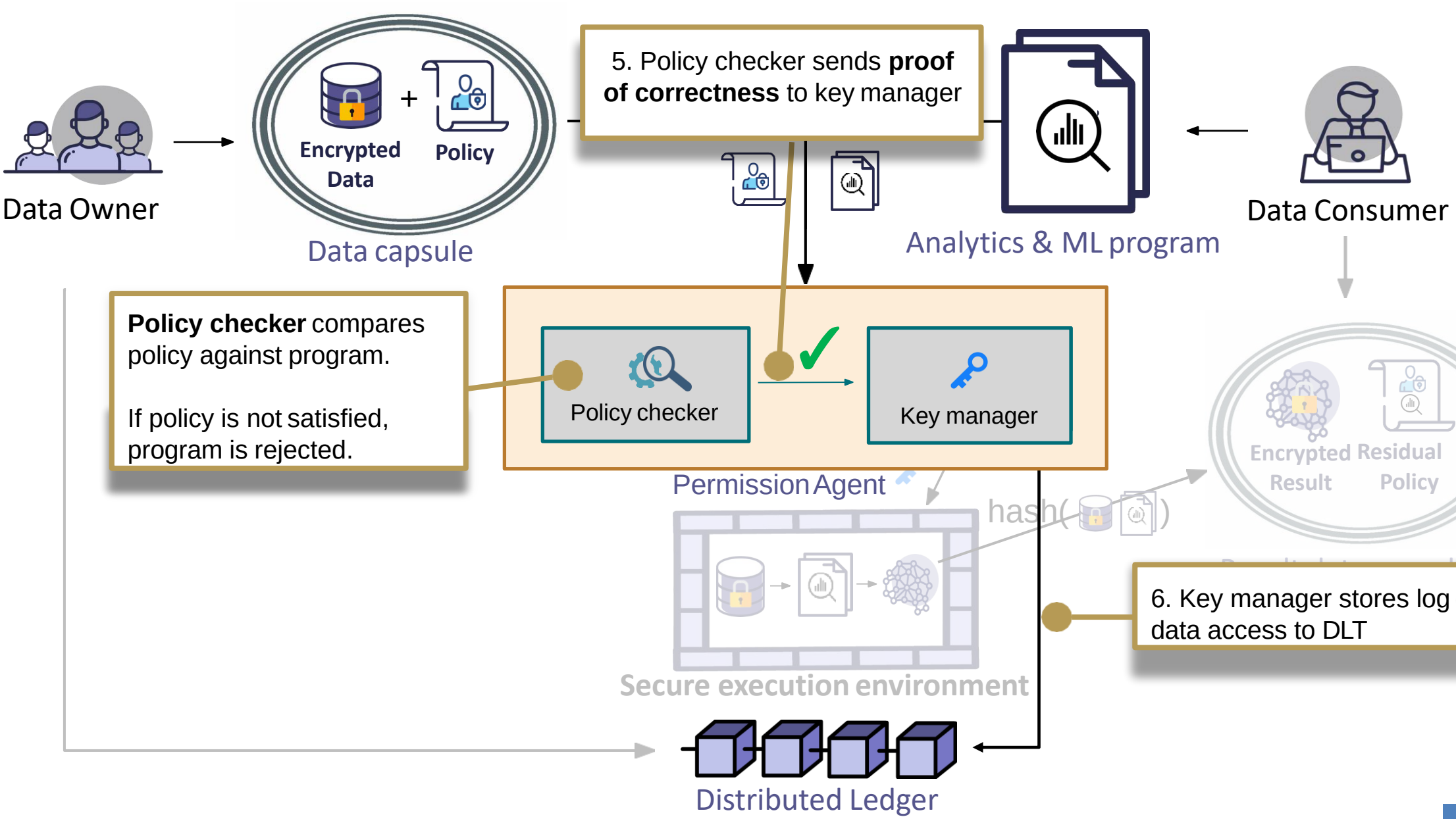
Result data capsule

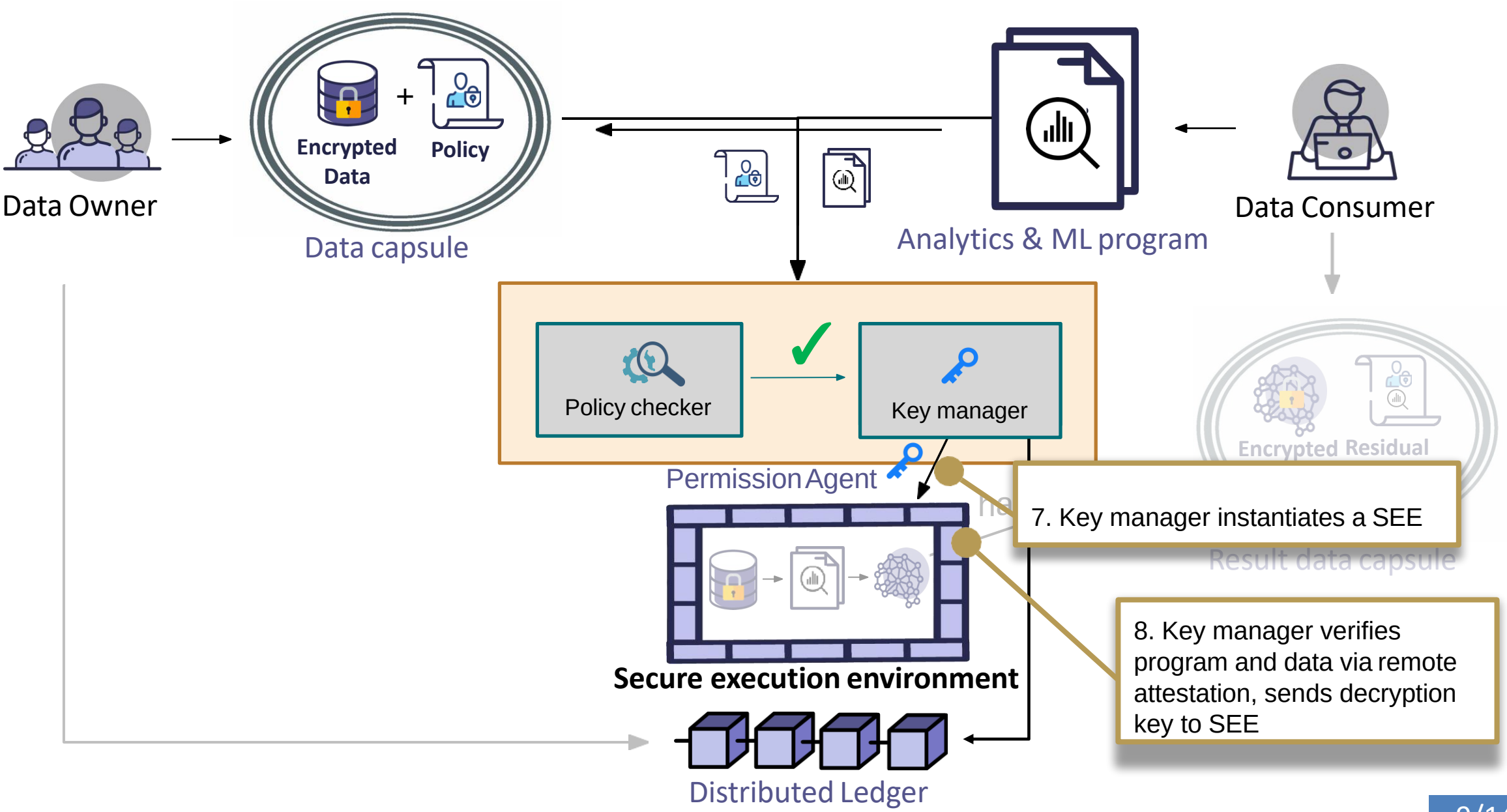


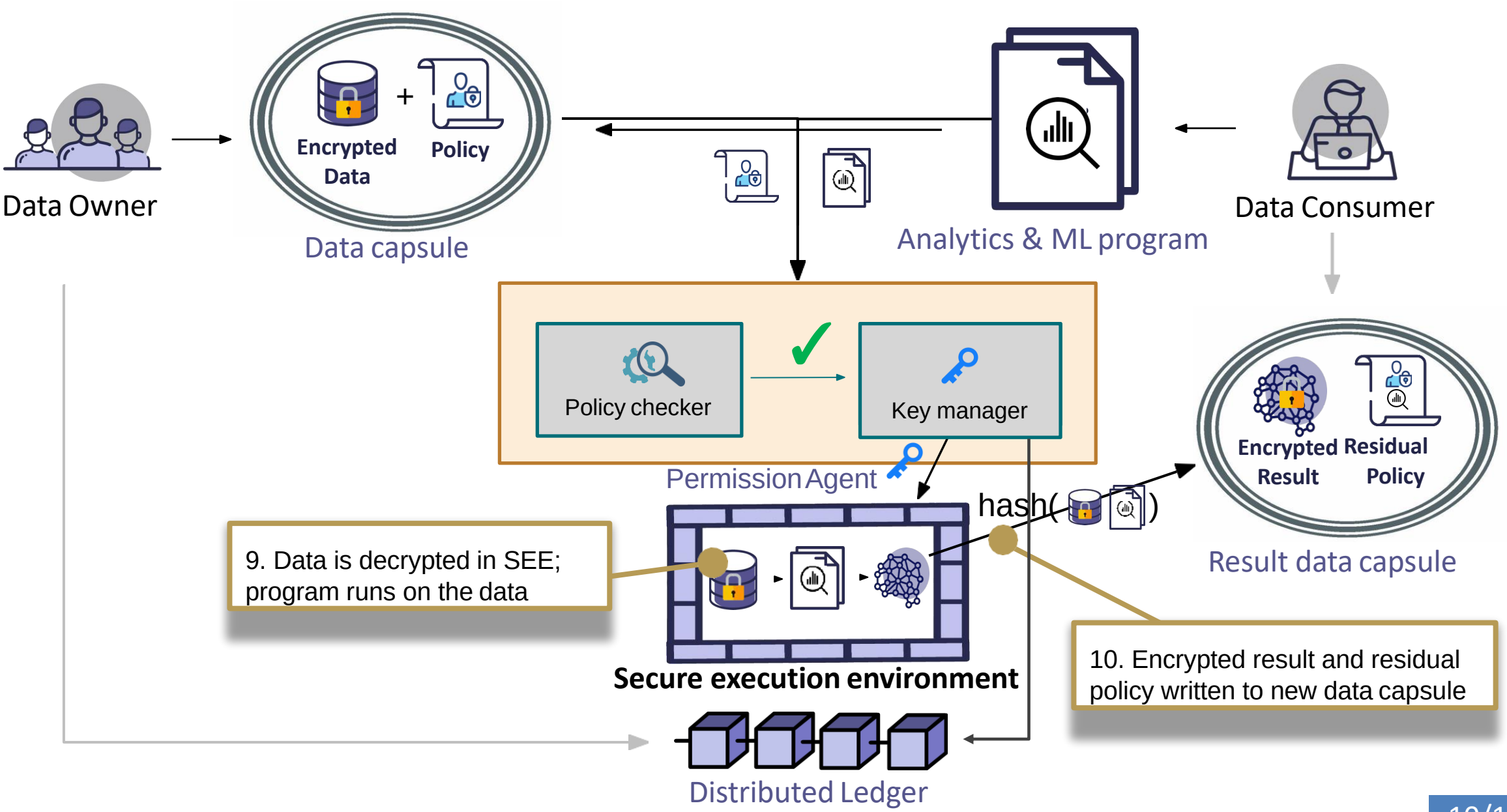
Distributed Ledger

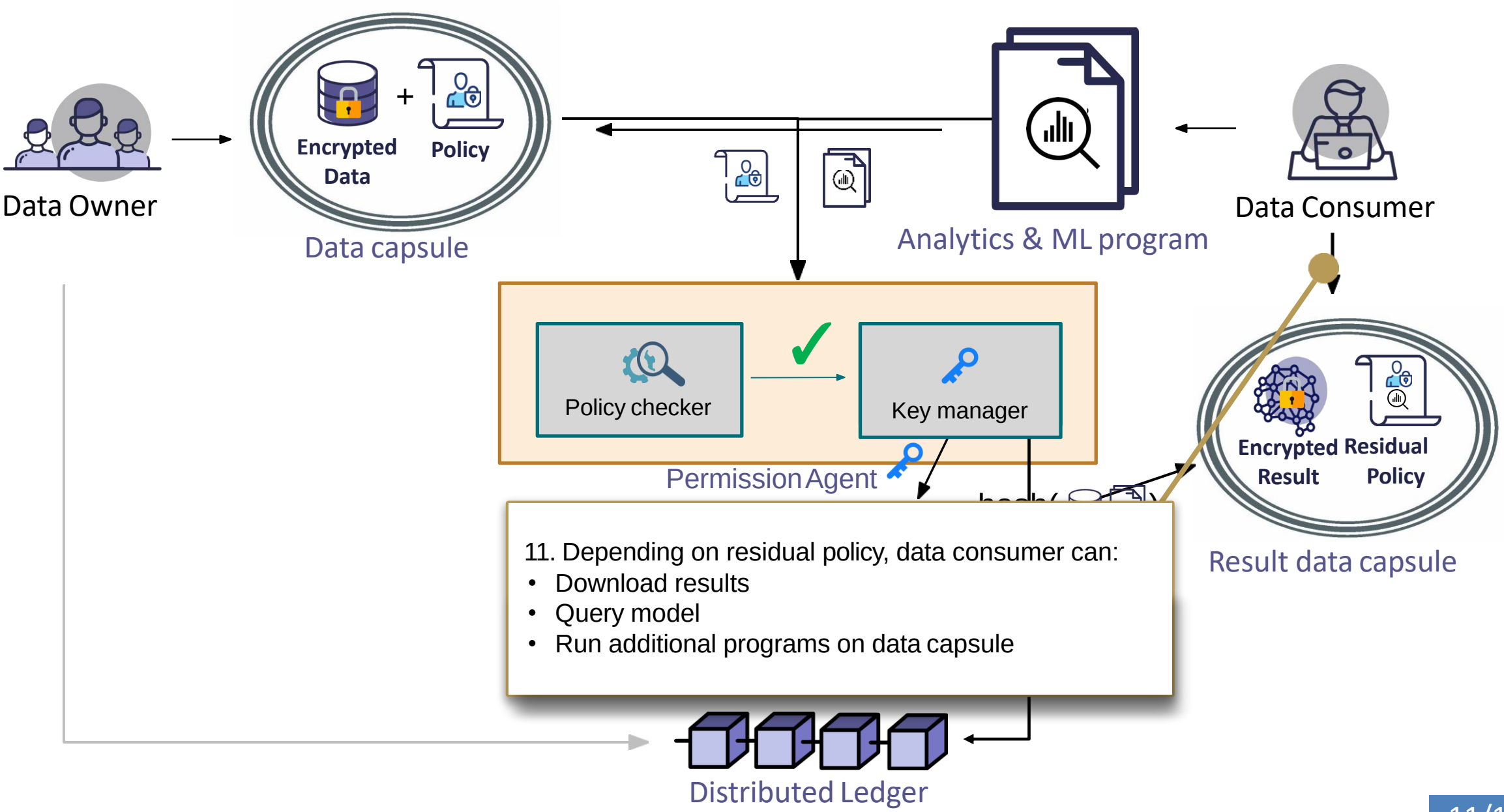

1. Data provider bundles data and policy into a data capsule
3. Data consumer contract requests to run on data
2. Data consumer submits program
Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker
Key manager
Permission Agent
hash( )
Encrypted Result
Residual Policy
Result data capsule
Secure execution environment
Distributed Ledger

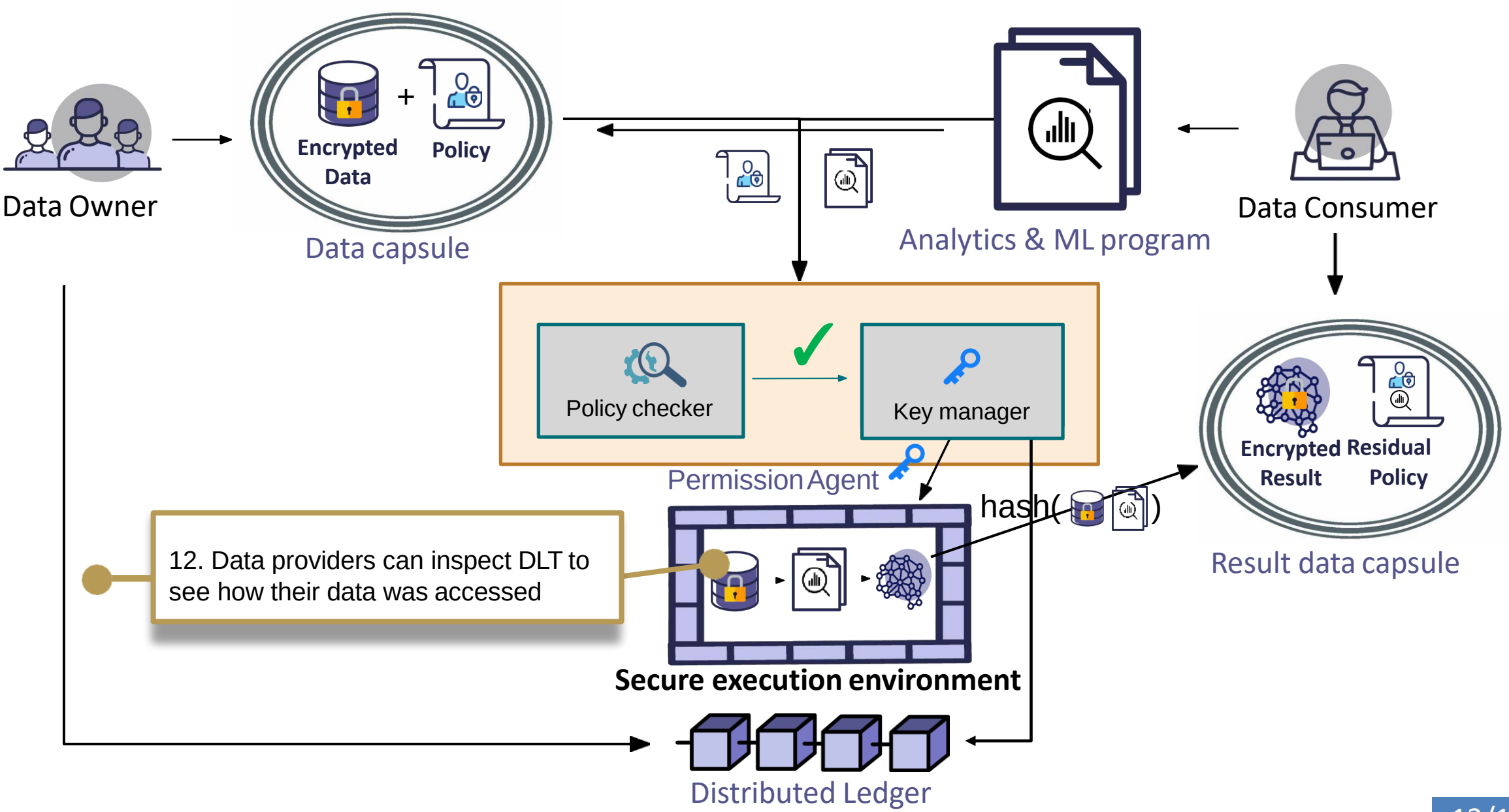

4. Program and policy are sent to **Permission Agent**
Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker compares policy against program.
If policy is not satisfied, program is rejected.
Policy checker
Key manager
Permission Agent
hash( )
Encrypted Result
Residual Policy
Result data capsule
Secure execution environment
Distributed Ledger


Data Owner
Encrypted Data
Policy
Data capsule
5. Policy checker sends **proof of correctness** to key manager
Analytics & ML program
Data Consumer
Policy checker compares policy against program.
If policy is not satisfied, program is rejected.
Policy checker
Key manager
Permission Agent
Encrypted Result
Residual Policy
hash( )
6. Key manager stores log of data access to DLT
Secure execution environment
Distributed Ledger


Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker
Key manager
Permission Agent
Encrypted Residual
Result data capsule
7. Key manager instantiates a SEE
8. Key manager verifies program and data via remote attestation, sends decryption key to SEE
Secure execution environment
Distributed Ledger


Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker
Key manager
Permission Agent
Encrypted Result
Residual Policy
Result data capsule
hash( )
9. Data is decrypted in SEE; program runs on the data
Secure execution environment
10. Encrypted result and residual policy written to new data capsule
Distributed Ledger


Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker
Key manager
Permission Agent
Encrypted Result
Residual Policy
Result data capsule
11. Depending on residual policy, data consumer can:
• Download results
• Query model
• Run additional programs on data capsule
Distributed Ledger

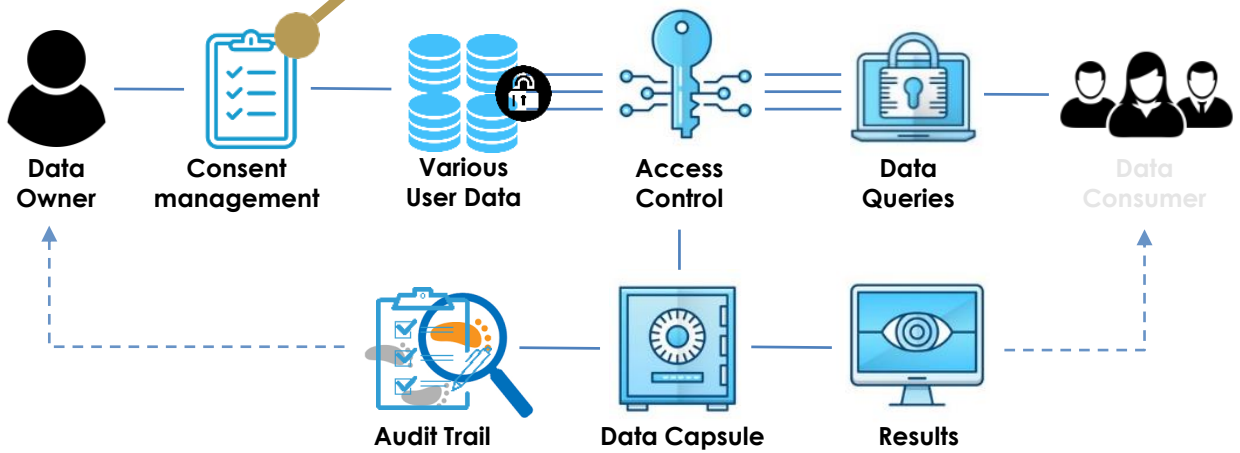

Data Owner
Encrypted Data
Policy
Data capsule
Analytics & ML program
Data Consumer
Policy checker
Key manager
Permission Agent
Encrypted Result
Residual Policy
Result data capsule
hash( )
12. Data providers can inspect DLT to see how their data was accessed
Secure execution environment
Distributed Ledger

Consent Management Solution

Solution to aggregating Data

With High Security and Low latency

13. User Interface to customize permissions and get control of data



User Privacy Act

CCPA and GDPR Compliance

CCPA

- Gain user consent before data collection
- Access Information:
  - User can see **"Who, What & Why"** to data
  - User can access to collected data
- Request Verification to prevent fraud
- Deletion of Information upon user request
- Opt-Out to sell data to third parties

Hybrid Block Chain

Storing Data off-chain to prevent scale problem

Create Data Capsule

decrypt and aggregate datasets and apply query

Consent Management

Access Control Policies (User & Company)

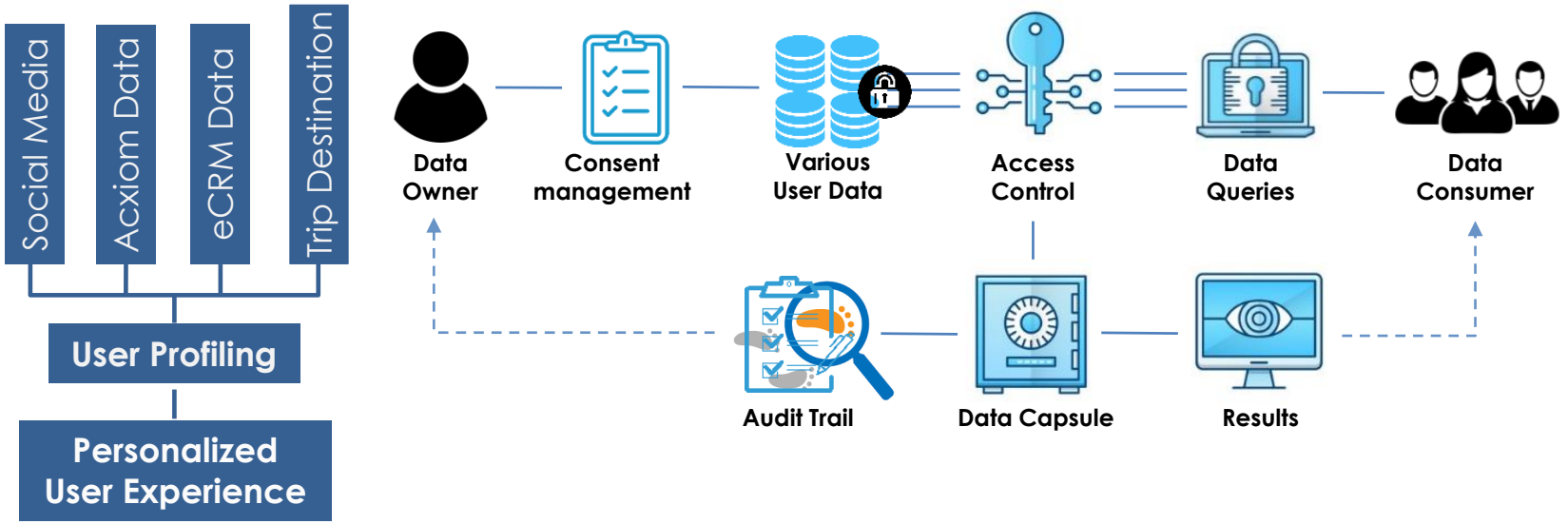
Audit Trail for data Capsule

Request, grant, and access are maintained in BC

Consent Management Solution

Solution to aggregating Data

With High Security and Low latency



User Privacy Act

CCPA and GDPR Compliance

CCPA

- Gain user consent before data collection
- Access Information:
  - User can see **"Who, What & Why"** to data
  - User can access to collected data
- Request Verification to prevent fraud
- Deletion of Information upon user request
- Opt-Out to sell data to third parties

Hybrid Block Chain

Storing Data off-chain to prevent scale problem

Create Data Capsule

decrypt and aggregate datasets and apply query

Consent Management

Access Control Policies (User & Company)

Audit Trail for data Capsule

Request, grant, and access are maintained in BC