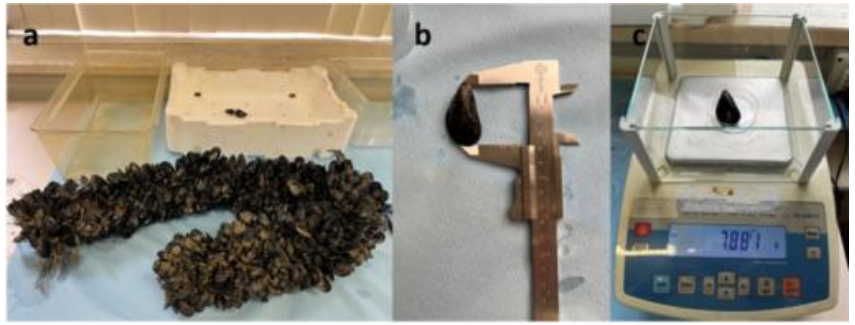
DII
Dipartimento di Ingegneria
dell'Informazione

A flexible and easy-to-use system for blockchain-based certification and traceability

Giacomo Zonneveld, Giulia Rafaiani, Franco Chiaraluce, Marco Baldi
Department of Information Engineering
Università Politecnica delle Marche

FOLOU project

- Main project objectives:
  - measure and estimate food losses (agriculture, aquaculture, and fisheries)
  - monitor and report food losses at Member States and European levels;
- Our contribution:
  - design and development of a blockchain-based platform to certify data
  - certification of the different processes involved in the case study related to mussel aquaculture



This project has received funding from the European Union's Horizon Europe research and innovation programme under grant agreement No 101084106

Target

BLOCKCHAIN-BASED TRACEABILITY

FLEXIBILITY AND EASE OF USE

COST-OPTIMIZED SOLUTION

ON-CHAIN/OFF-CHAIN STORAGE TRADE-OFF

System requirements and features

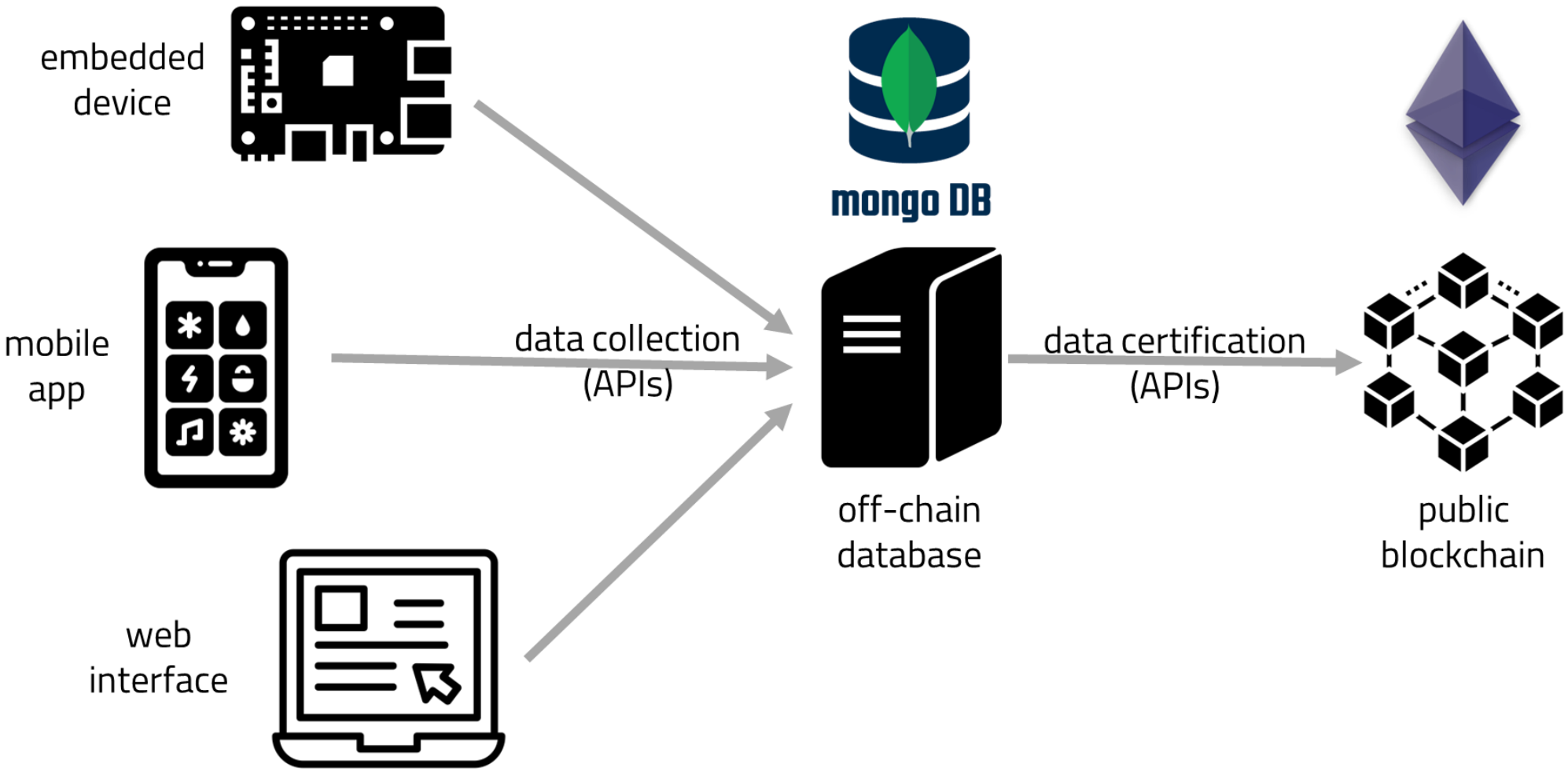
Data-Independent Approach
Multiple formats supported (Text, Number, Date, PDF, JSON, etc.)

User-friendly interface
(web-based)

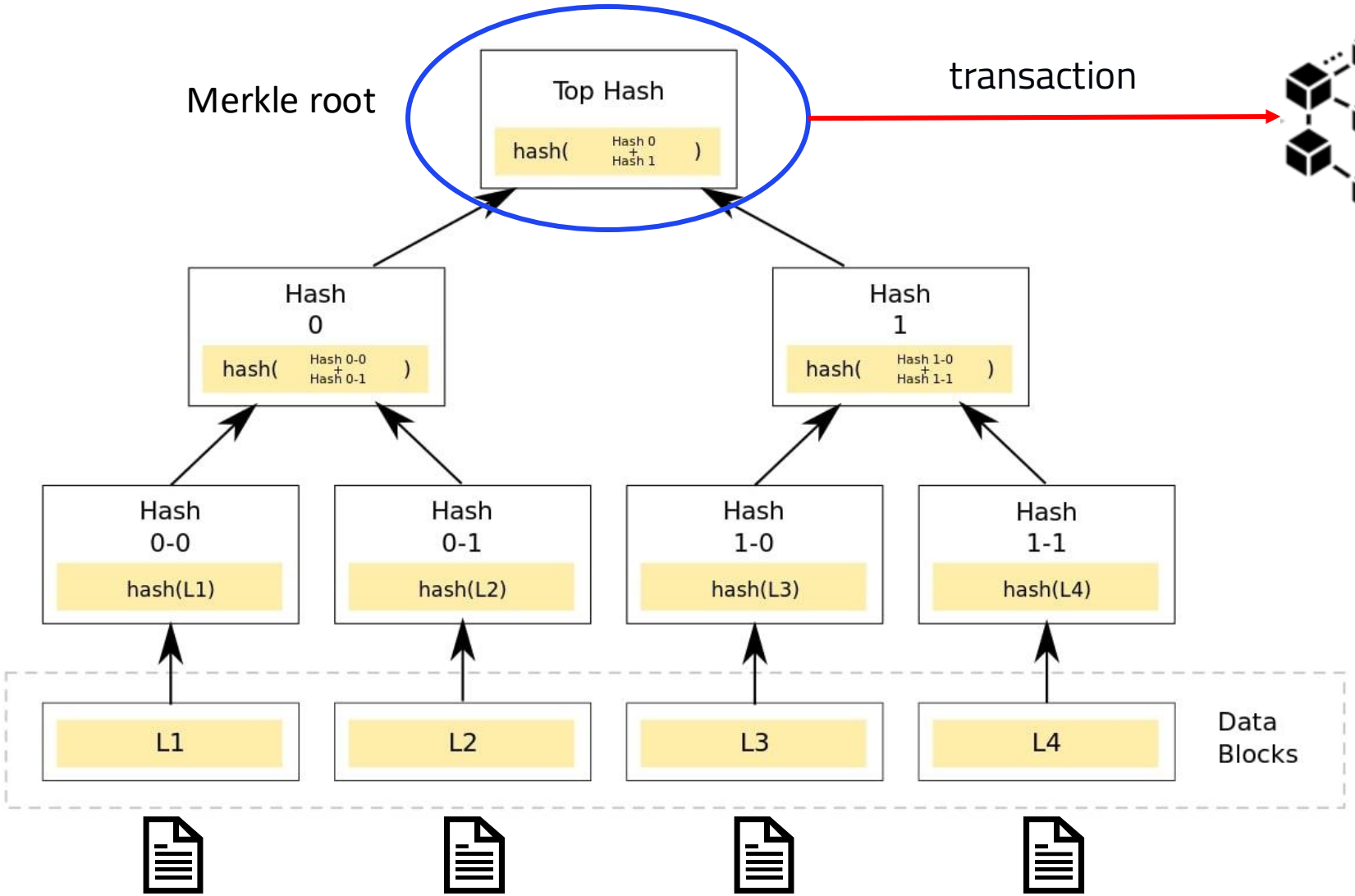
Option to ensure data confidentiality
Data owners can choose if certified data is publicly available or not

Reference to a specific supply chain

Outline of the data certification infrastructure

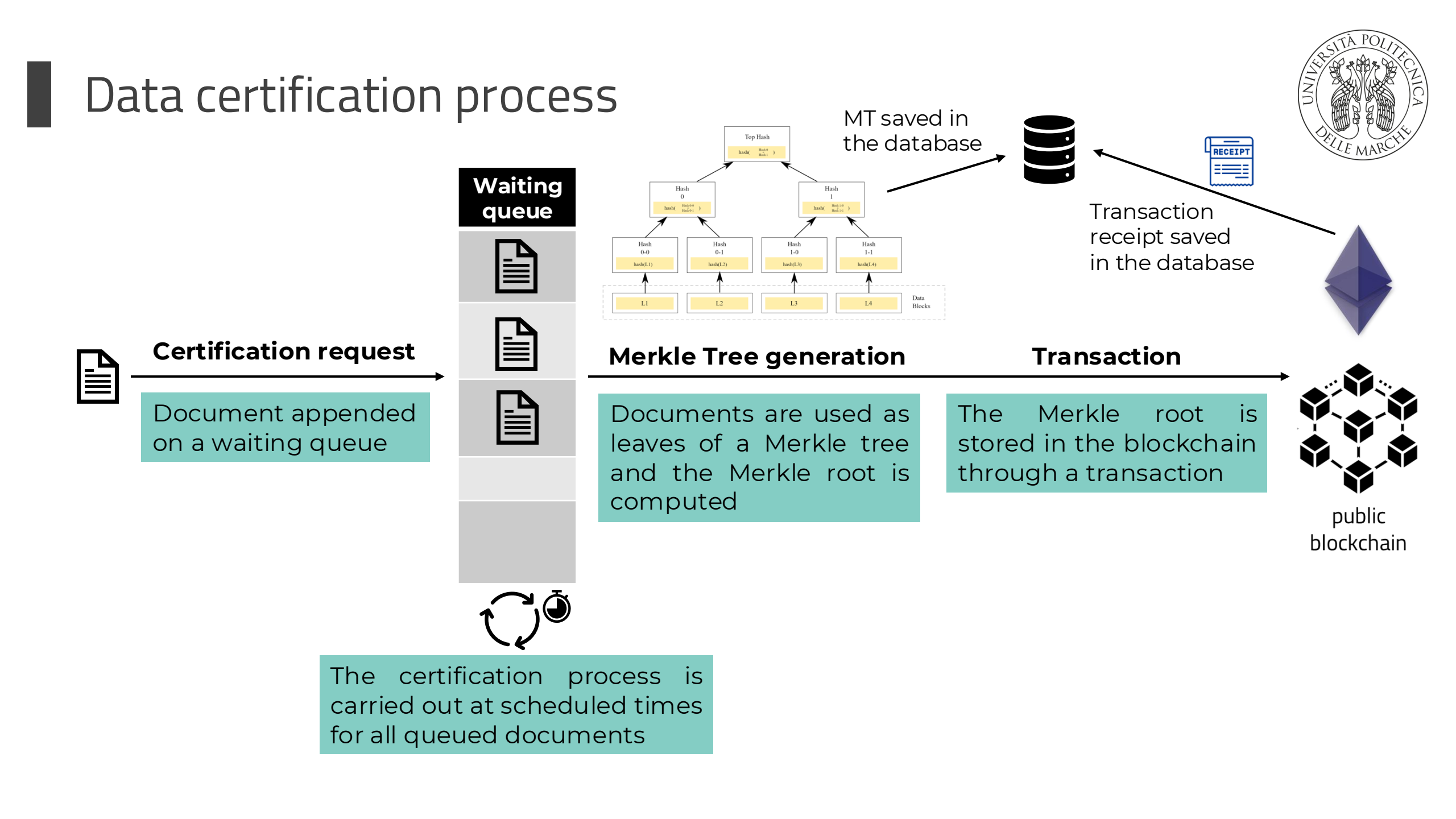


Data certification (through Merkle trees)



Multiple data, one transaction

Data certification process



Document appended on a waiting queue

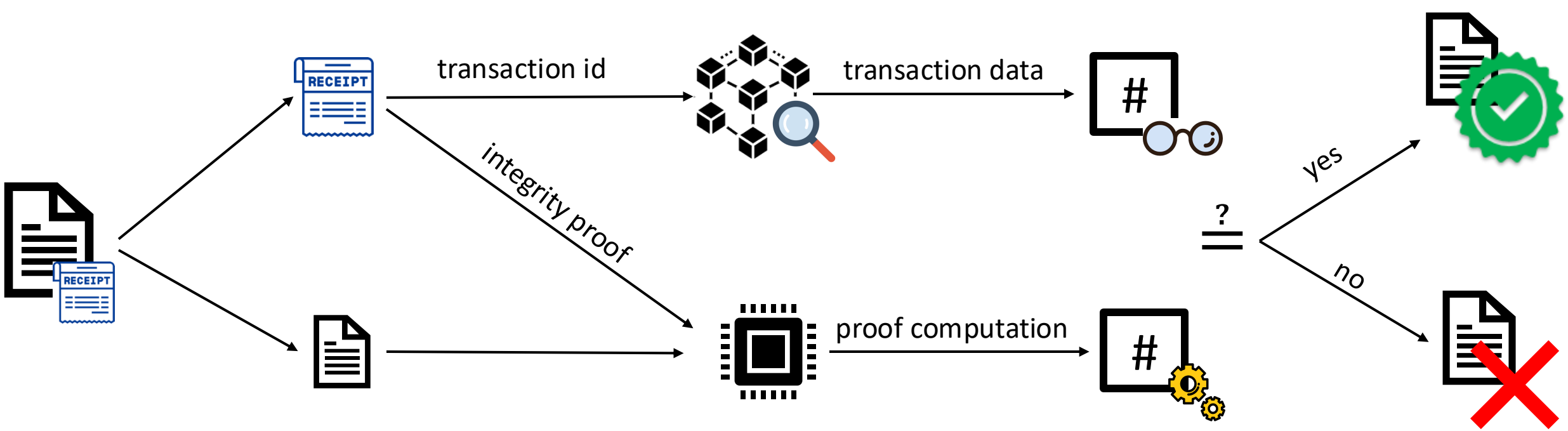
Documents are used as leaves of a Merkle tree and the Merkle root is computed

The Merkle root is stored in the blockchain through a transaction

The certification process is carried out at scheduled times for all queued documents

Data verification process

Blockchain is explored to **read the Merkle root** previously stored with a transaction



Information extraction

Separation of transaction receipt from certified data

Merkle root computation

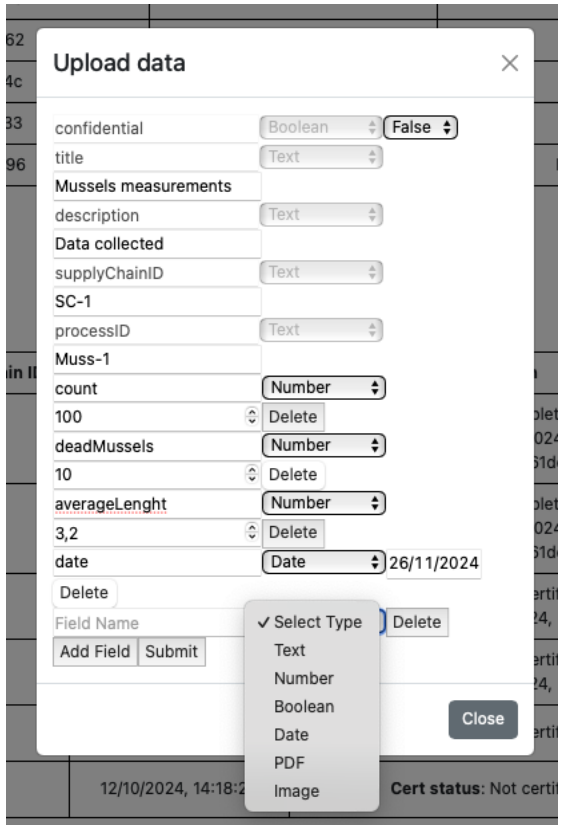
Using the integrity proof and the certified data, the **Merkle root is computed locally**.

Merkle roots comparison

The comparison determines the validity of the given data

Workflow summarised

Data Uploading



Certification request

Multiple data can be added to the certification queue.

Requests can be aborted until certification procedure is started.

Certification on blockchain

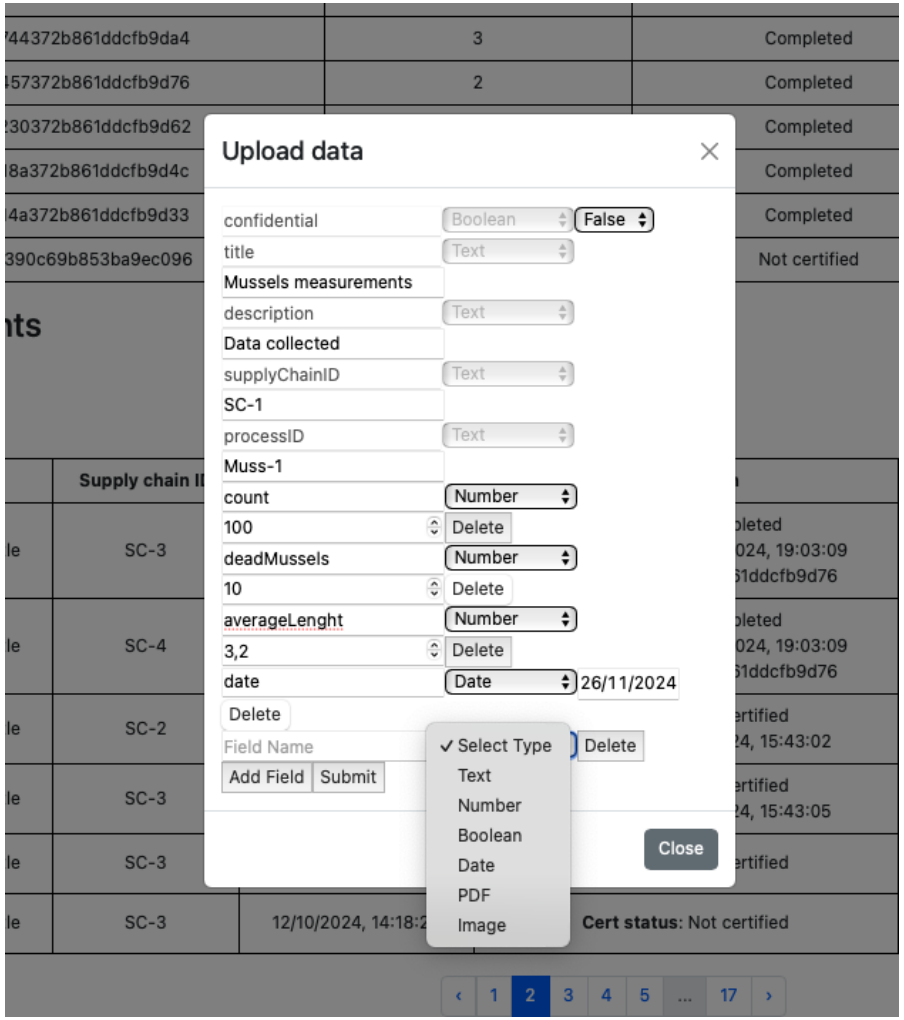
Transaction contains compressed information on data to be certified.

Single transaction for multiple data

Verification of data integrity

Once the transaction has been accepted by the network, data integrity is verifiable forever

Uploading of data to be certified



Customizable fields

- User can decide which data must be uploaded
- Presence of mandatory fields can be enforced
  - Example: Supply chain ID, data confidentiality
- For each field some information must be defined:
  - Field name
  - Data type
  - Value

Data management and certification

Folou

Staff - Documents

All certifications

Ticket	N. of documents	Certification status	Certification timestamp
673e2744372b861ddcfb9da4	3	Completed	20/11/2024, 20:59:31
673e2457372b861ddcfb9d76	2	Completed	20/11/2024, 19:03:09
673e2230372b861ddcfb9d62	1	Completed	20/11/2024, 18:59:39
673e218a372b861ddcfb9d4c	2	Completed	20/11/2024, 18:51:13
673e214a372b861ddcfb9d33	3	Completed	20/11/2024, 18:50:09
6746f0390c69b853ba9ec096	6	Not certified	

My Documents

Upload data

Title	Supply chain ID	Upload timestamp	Certification	Actions
A comprehensive title	SC-3	29/10/2024, 13:15:55	**Cert status**: Completed **Transaction date**: 20/11/2024, 19:03:09 **Ticket**: 673e2457372b861ddcfb9d76	Data Details Cert Info
A comprehensive title	SC-4	27/10/2024, 02:21:10	**Cert status**: Completed **Transaction date**: 20/11/2024, 19:03:09 **Ticket**: 673e2457372b861ddcfb9d76	Data Details Cert Info
A comprehensive title	SC-2	19/10/2024, 05:10:50	**Cert status**: Not certified **Request date**: 27/11/2024, 15:43:02	Data Details Abort
A comprehensive title	SC-3	18/10/2024, 17:43:24	**Cert status**: Not certified **Request date**: 27/11/2024, 15:43:05	Data Details Abort
A comprehensive title	SC-3	17/10/2024, 17:30:41	**Cert status**: Not certified	Data Details Certify Delete Edit
A comprehensive title	SC-3	12/10/2024, 14:18:28	**Cert status**: Not certified	Data Details Certify Delete Edit

‹ 1 2 3 4 5 ... 17 ›

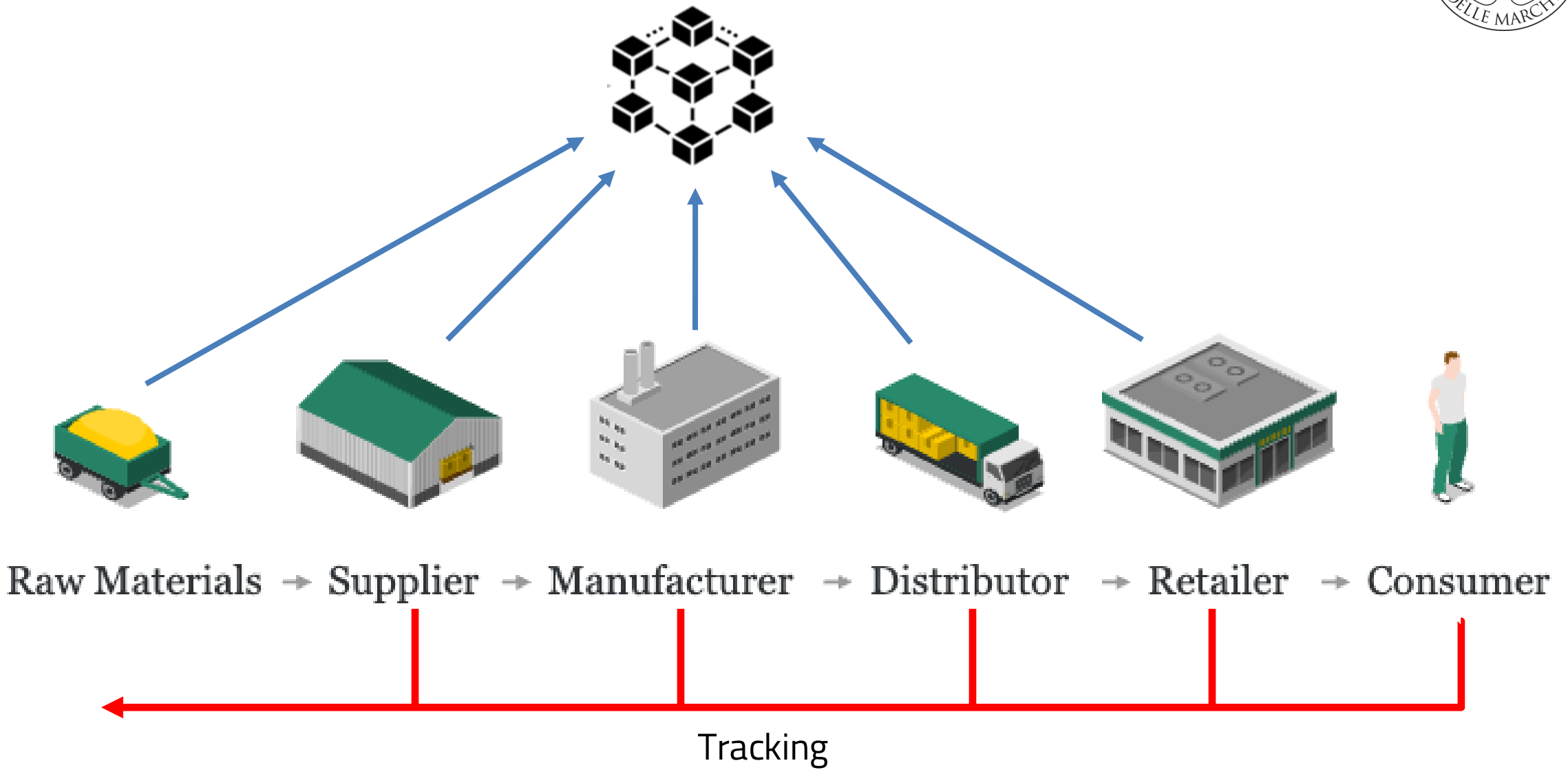
Transaction information available

- Certification status
- Transaction timestamp
- Number of documents certified in each stack

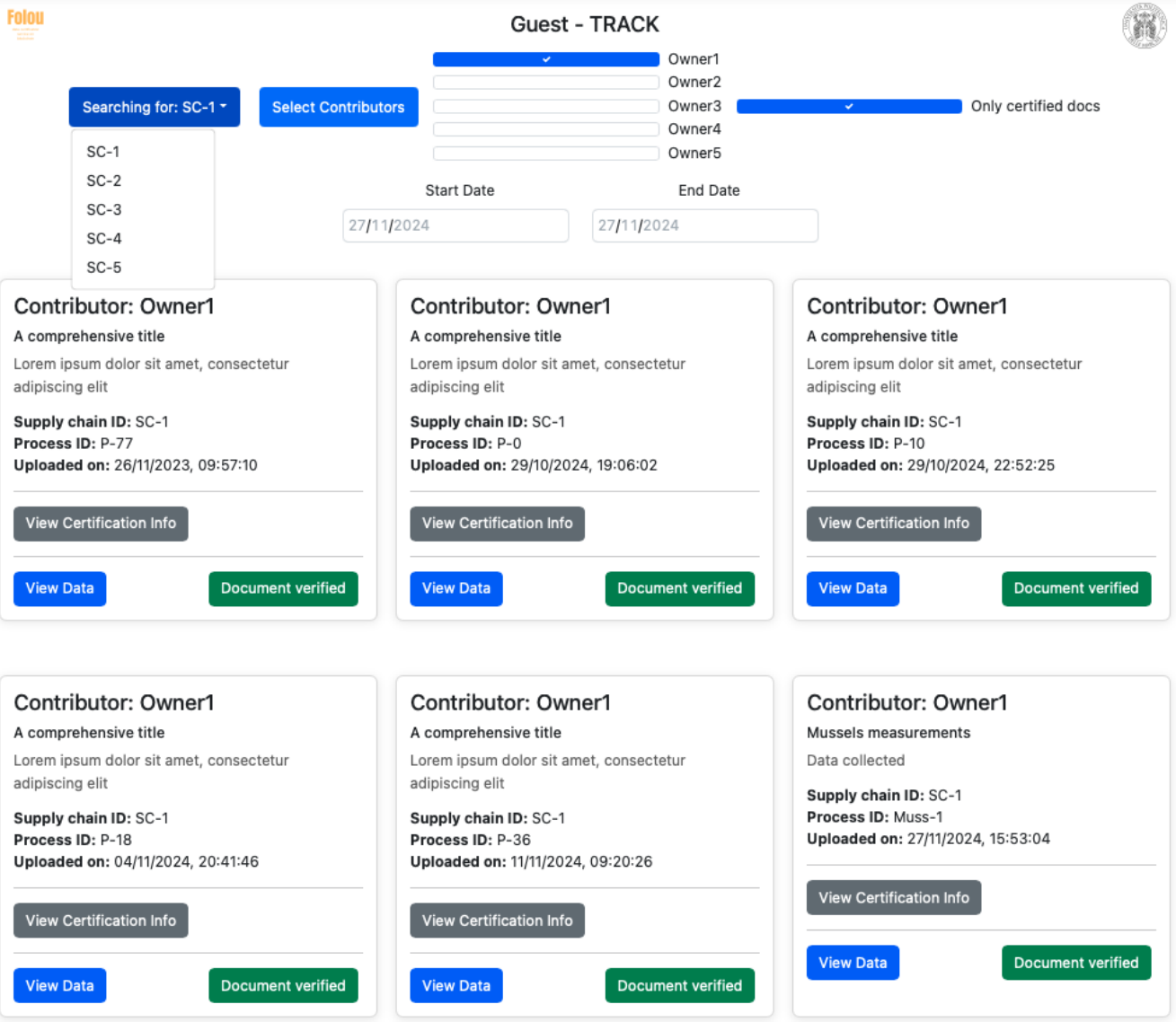
Once certified, data can no longer be changed

Once a certification request has been submitted, it's only possible to **view the data** or **abort the request**.

Traceability



Supply Chain Tracking

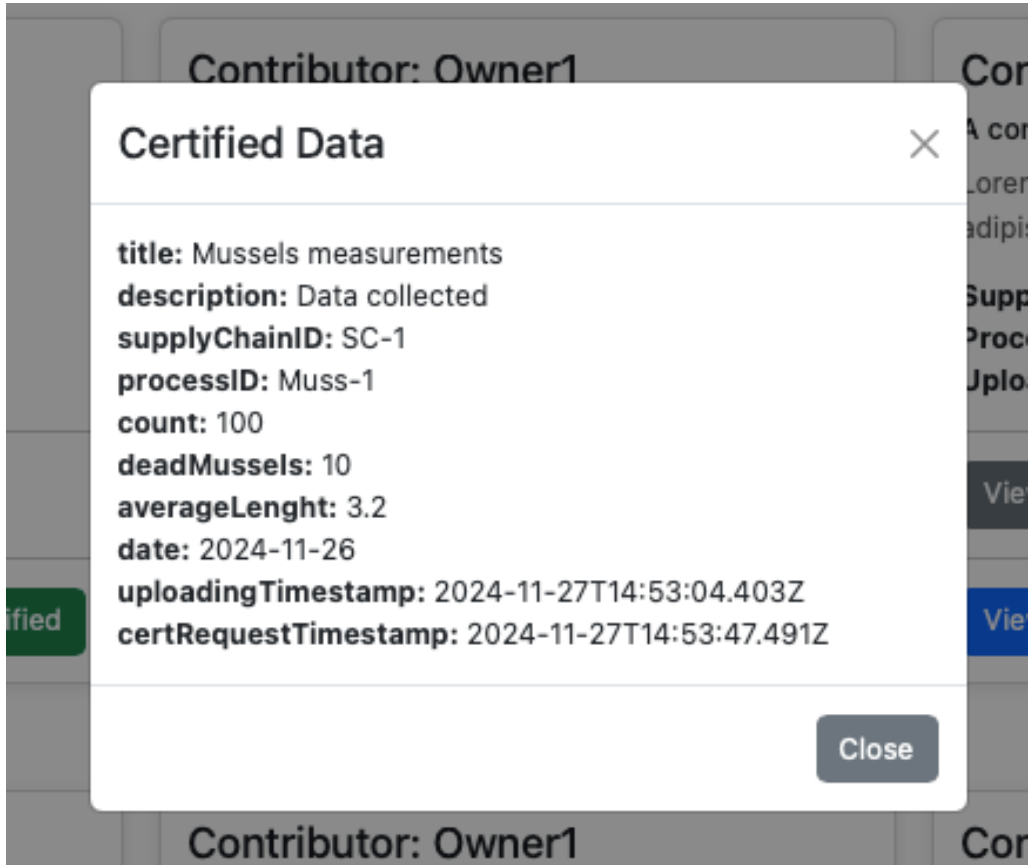


Visitors can **traverse the supply chain** to view all published data

Multiple filters can be applied

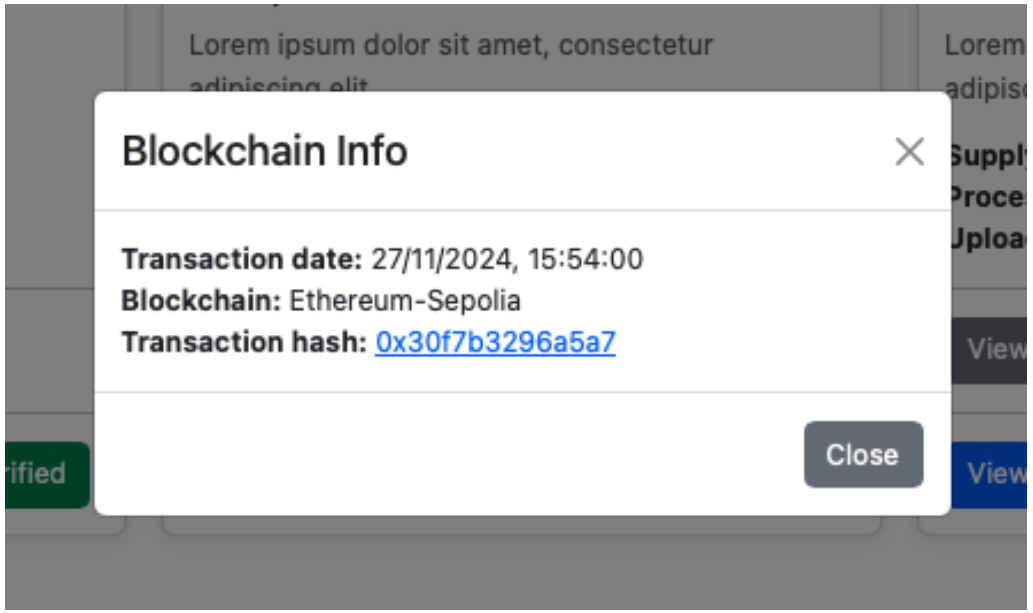
- Specify the supply chain of interest
- Select contributors (who uploaded data)
- View only certified data
- Define an uploading time window

Supply Chain Tracking



Visitors can view

- Certified data
- Transaction information



SCAN ME

Existing standard: Chainpoint

- Open standard for creating a timestamp proof of any data, file or process
- Currently on version 2 and version 3 scheduled for future release
- It formalizes the structure of an integrity proof based on the use of Merkle trees
- Difficult to adapt to scenarios where the hashing operation on data to be certified is not straightforward
  - For integrity verification its required that the hash of the certified data is computed on the fly
  - On Chainpoint it is reported as part of the integrity proof

EXAMPLE


```
{
  "@context": "https://w3id.org/chainpoint/v2",
  "type": "ChainpointSHA256v2",
  "targetHash": "bdf8c9bdf076d6aff0292a1c9448691d2ae283f2ce41b045355e2c8cb8e85ef2",
  "merkleRoot": "51296468ea48ddbcc546abb85b935c73058fd8acdb0b953da6aa1ae966581a7a",
  "proof": [
    {
      "left": "bdf8c9bdf076d6aff0292a1c9448691d2ae283f2ce41b045355e2c8cb8e85ef2"
    },
    {
      "left": "cb0dbbedb5ec5363e39be9fc43f56f321e1572cfcf304d26fc67cb6ea2e49faf"
    },
    {
      "right": "cb0dbbedb5ec5363e39be9fc43f56f321e1572cfcf304d26fc67cb6ea2e49faf"
    }
  ],
  "anchors": [
    {
      "type": "BTCOpReturn",
      "sourceId": "f3be82fe1b5d8f18e009cb9a491781289d2e01678311fe2b2e4e84381aafadee"
    }
  ]
}
```

UNIVERSITÀ
POLITECNICA
DELLE MARCHE

DII
Dipartimento di Ingegneria
dell'Informazione

Thanks for the attention

Giacomo Zonneveld

g.zonneveld@univpm.it