

CAKE and MARTSIA: Fine-Grained Data Sharing in Blockchain Applications and Business Processes

Ingo Weber – TUM and Fraunhofer

Edoardo Marangone – Computer Science Department Sapienza
University of Rome – edoardo.marangone@uniroma1.it

Acknowledgement: **exPlainable kNowledge-aware PrOcess INTelligence**. PINPOINT is a project funded by MIUR under the PRIN 2020 initiative (grant **B87G22000450001**)

<https://pinpoint.unibz.it/>



Introduction

- Building on blockchain technology
- Default use case: business processes involving multiple parties
 - But many parts of our tech can be used for general-purpose Dapps
- Transparency: copy of the ledger, data freely accessible*
*within the network
- Security / confidentiality / privacy issue:
 - All-or-nothing read access of on-chain data
 - Goal: confidential / commercial-in-confidence data should be only readable for authorized entities

Objectives

1. Guarantee data privacy among parties
2. Let parties exchange information in a secure way
3. Let parties hide data (or parts thereof) from other players

While collaborators cooperate...

Public
permissionless
platforms are
more **robust** and
guarantee
non-repudiation



Every participant
in the public
blockchain
network can **read**
the data

... the whole network observes

Public
permissionless
platforms are
more **robust** and
guarantee
non-repudiation



What about
confidentiality?

Every participant
in the public
blockchain
network can **read**
the data

Example

Actors

- Manufacturer



- National customs



- International customs



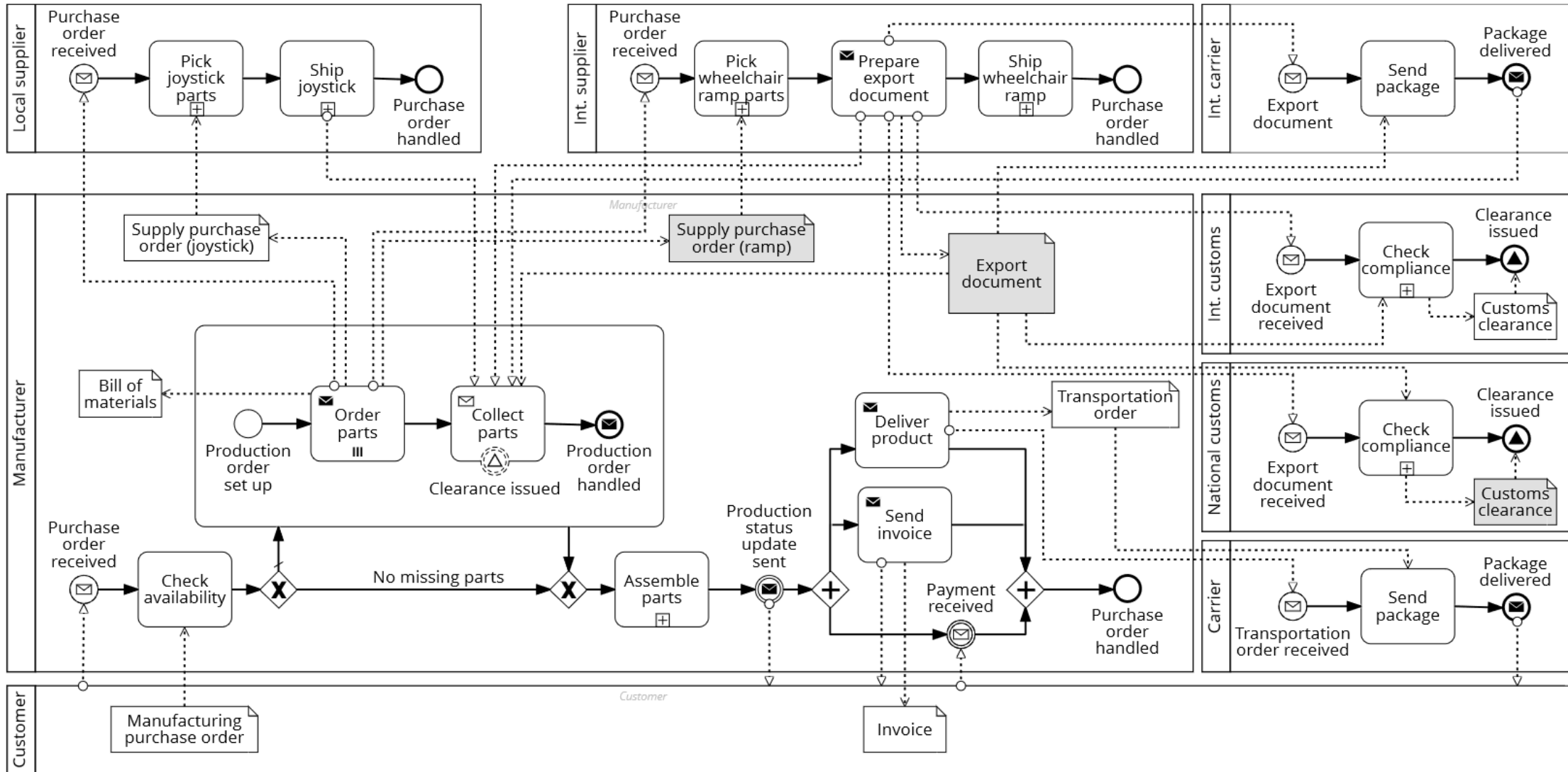
- International carrier



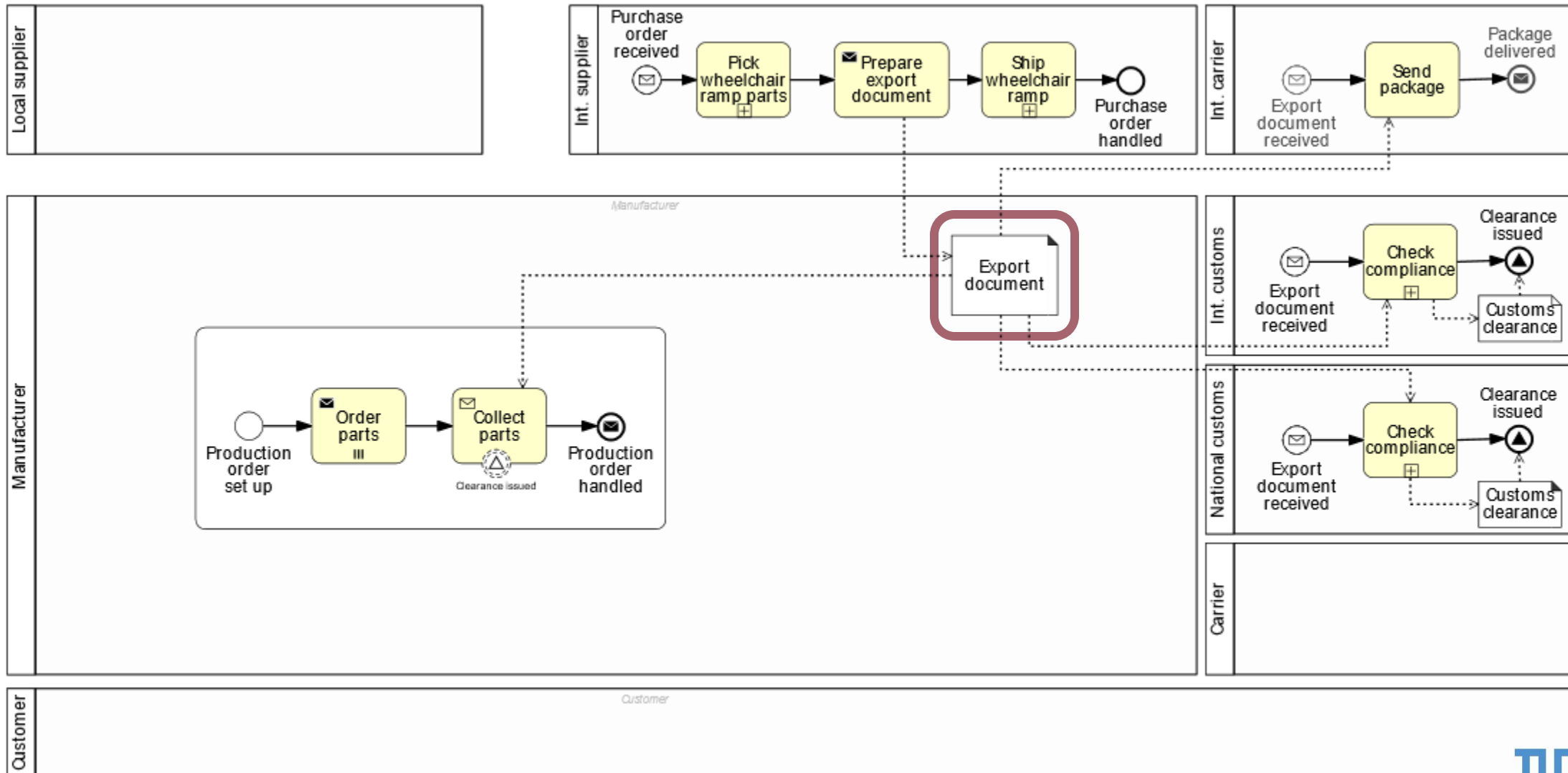
- International supplier



Business Process Model and Notation (BPMN) collaboration diagram



Business Process Model and Notation (BPMN) collaboration diagram

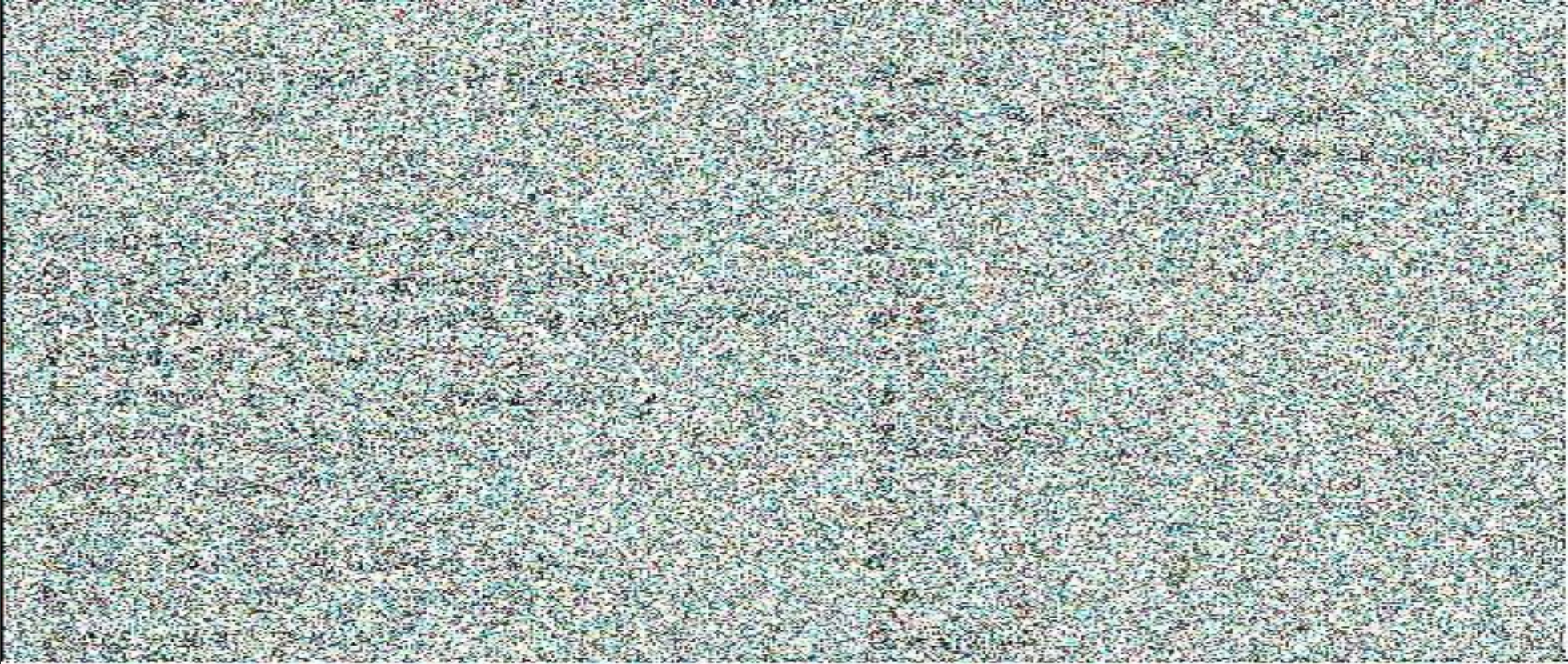


The message, in clear (as seen by the international supplier)

Message	Sender	Data	Recipients
Export document	International supplier	Manufacturer_company: Beta Delivery_address: 82, Beta street E-mail: mnfctr.beta@mail.com Ramp_run: 3 Kickplate: 12 Handrail: 7 Baluster: 30 Guardrail: 25 Amount_paid: \$5000	Manufacturer National customs International customs International carrier
		Fundamental_workers_rights: Ok Human_rights: Ok Protection_biodiversity_and_ecosystems: Ok Protection_water_and_air: Ok Combatting_climate_change: Ok	National customs International customs
		Manufacturer_company: Beta Address: 78, Beta street Order_reference: 26487	Manufacturer
		Invoice_ID: 101711 Billing_address: 34, Gamma street Gross_total: \$5000 Company_VAT: U12345678 Issue_date: 2022-05-12	Manufacturer National customs International customs



The message (as seen by external parties)

Message	Sender	Data	Recipients
			

The message (as seen by the manufacturer)



Message	Sender	Data	Recipients
Export document	International supplier	Manufacturer_company: Beta Delivery_address: 82, Beta street E-mail: mnfctr.beta@mail.com Ramp_run: 3 Kickplate: 12 Handrail: 7 Baluster: 30 Guardrail: 25 Amount_paid: \$5000	Manufacturer National customs International customs International carrier
		Manufacturer_company: Beta Address: 78, Beta street Order_reference: 26487	Manufacturer
		Invoice_ID: 101711 Billing_address: 34, Gamma street Gross_total: \$5000 Company_VAT: U12345678 Issue_date: 2022-05-12	Manufacturer National customs International customs

The message (as seen by the international carrier)



Message	Sender	Data	Recipients
Export document	International supplier	Manufacturer_company: Beta Delivery_address: 82, Beta street E-mail: mnfctr.beta@mail.com Ramp run: 3 Kickplate: 12 Handrail: 7 Baluster: 30 Guardrail: 25 Amount_paid: \$5000	Manufacturer National customs International customs International carrier

Hence the name: CAKE - Control Access via Key Encryption



Control Access via Key Encryption (CAKE)

1. Edoardo Marangone, Claudio Di Ciccio, and Ingo Weber. 2022. Fine-Grained Data Access Control for Collaborative Process Execution on Blockchain. In BPM Blockchain and RPA Forum. Springer, 51–67. https://doi.org/10.1007/978-3-031-16168-1_4
2. Edoardo Marangone, Michele Spina, Claudio Di Ciccio, Ingo Weber. 2024. CAKE: Sharing Slices of Confidential Data on Blockchain. In Intelligent Information Systems. CAiSE 2024. Lecture Notes in Business Information Processing, vol 520. Springer, Cham. https://doi.org/10.1007/978-3-031-61000-4_16

Ingredients

- Blockchains (EVM)
- Smart Contracts
- InterPlanetary File System (IPFS)
- Attribute-Based Encryption (ABE): Ciphertext-Policy ABE (CP)

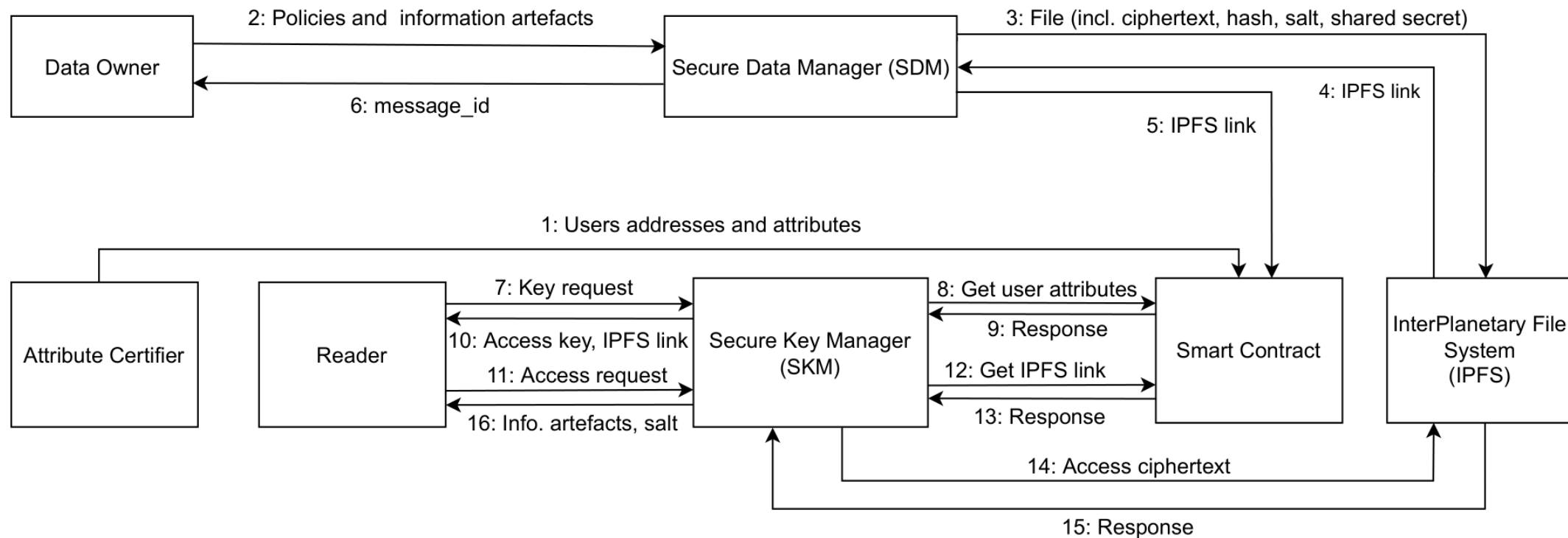
InterPlanetary File System (IPFS)

- Distributed system for the storage and access to files
- No central authority
- Content-addressing to uniquely identify each file in the network
- Files scattered among several nodes (Merkle DAGs)
- Distributed Hash Table (DHT) at its core

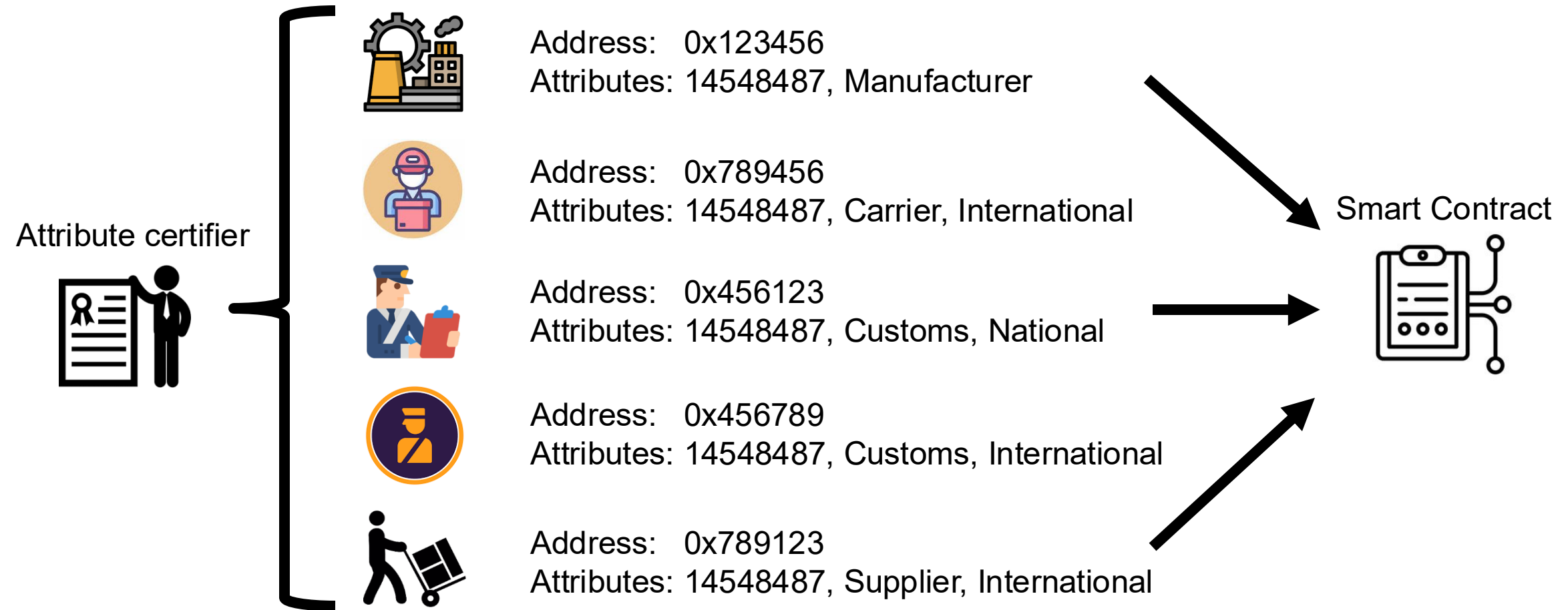
CP-ABE

- Attribute-Based Encryption (ABE): type of public-key encryption
- Ciphertext-Policy ABE (CP):
 - **Users** are associated with **attributes**
 - (propositional literals)
 - **Messages** are associated with **policies**
 - (propositional formulae on attributes)
- Attributes ex.: 14548487, Supplier, International, Manufacturer
- Policy ex.: 14548487 *and* (Manufacturer *or* (Supplier *and* International))

CAKE architecture



Pre-phase



Phase 1: ciphering

Original data	
Manufacturer_company:	Beta
Delivery_address:	82, Beta street
E-mail:	mnfctr.beta@mail.com
Ramp run:	3
Kickplate:	12
Handrail:	7
Baluster:	30
Guardrail:	25
Amount_paid:	\$5000
Fundamental_workers_rights:	Ok
Human_rights:	Ok
Protection_biodiversity_and_ecosystems:	Ok
Protection_water_and_air:	Ok
Combatting_climate_change:	Ok
Manufacturer_company:	Beta
Address:	78, Beta street
Order_reference:	26487
Invoice_ID:	101711
Billing_address:	34, Gamma street
Gross_total:	\$5000
Company_VAT:	U12345678
Issue_date:	2022-05-12

Customs or (14548487 and ((Supplier and International)
or Manufacturer or (Carrier and International)))

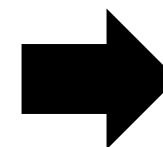
Customs or (14548487 and (Supplier and International))

14548487 and ((Supplier and International) or Manufacturer)

Customs or (14548487 and ((Supplier and International) or Manufacturer))

Phase 1: ciphering

File header	File body (slices)
	<pre>slice_id: 7816105805828306901, hash: 0x953a [...] f8d8, salt: "Zu00 [...] u004", metadata: {"c1": [...] 00a0}, cipherText: "oT2W [...] MQ=="</pre>
<pre>sender: 0x906D [...] Dba8, message_id: 17071949511205323542, pk: {"g": "\\u0087 [...] 00ca}, mk: {"beta": "\\u00b2 [...] 00fb}</pre>	<pre>slice_id: 6847895862959863592, hash: 0x12es [...] 1g23, salt: "bw32 [...] b464", metadata: {"c1": [...] asq2}, cipherText: "AS2w [...] btwd"</pre>
	<pre>slice_id: 3147899764966459866, hash: 0xj4rs [...] ne3d, salt: "ns1w [...] mey4", metadata: {"c1": [...] 23rs}, cipherText: "ht3r [...] asf3"</pre>
	<pre>slice_id: 12641782614493395949, hash: 0xad46 [...] 0f79, salt: "o9\u [...] 01e5, metadata: {"c1": [...] u09a}, cipherText: "7QsM [...] KVRs"</pre>



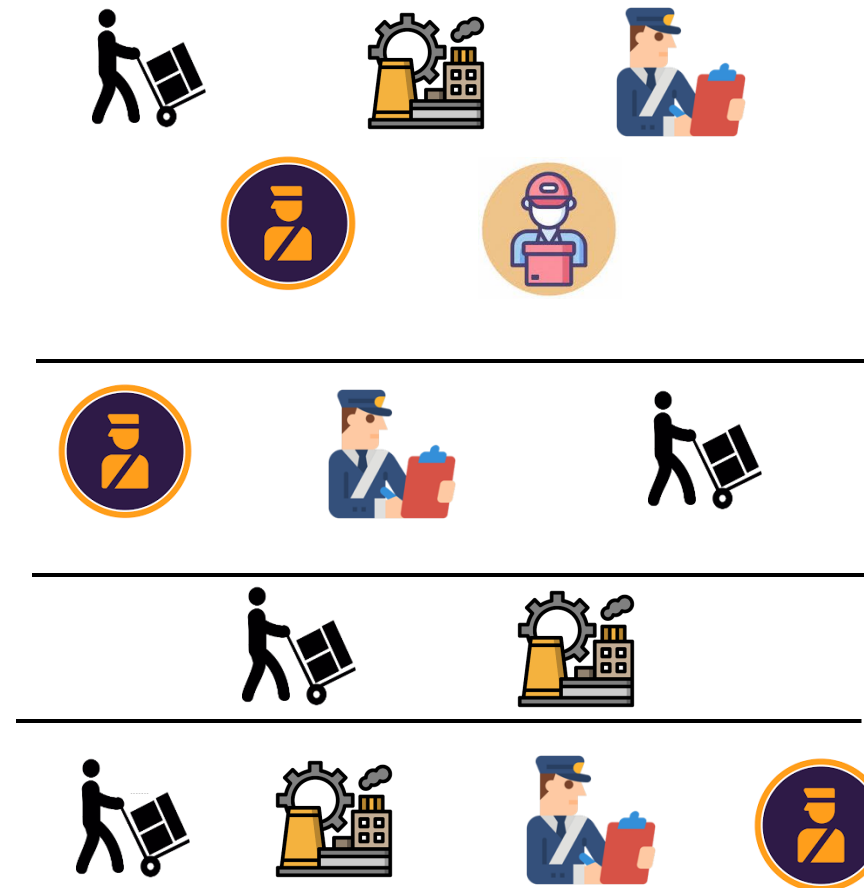
Phase 3: deciphering

File header	File body (slices)
	<pre>slice_id: 7816105805828306901, hash: 0x953a [...] f8d8, salt: "Zu00 [...] u004", metadata: {"c1": [...] 00a0}, cipherText: "oT2W [...] MQ=="</pre>
<pre>sender: 0x906D [...] Dba8, message_id: 17071949511205323542, pk: {"g": "\\u0087 [...] 00ca}, mk: {"beta": "\\u00b2 [...] 00fb}</pre>	<pre>slice_id: 6847895862959863592, hash: 0x12es [...] 1g23, salt: "bw32 [...] b464", metadata: {"c1": [...] asq2}, cipherText: "AS2w [...] btwd"</pre>
	<pre>slice_id: 3147899764966459866, hash: 0xj4rs [...] ne3d, salt: "ns1w [...] mey4", metadata: {"c1": [...] 23rs}, cipherText: "ht3r [...] asf3"</pre>
	<pre>slice_id: 12641782614493395949, hash: 0xad46 [...] 0f79, salt: "o9\u [...] 01e5, metadata: {"c1": [...] u09a}, cipherText: "7QsM [...] KQRS"</pre>



Phase 3: deciphering

Original data	
Manufacturer_company:	Beta
Delivery_address:	82, Beta street
E-mail:	mnfctr.beta@mail.com
Ramp run:	3
Kickplate:	12
Handrail:	7
Baluster:	30
Guardrail:	25
Amount_paid:	\$5000
Fundamental_workers_rights:	Ok
Human_rights:	Ok
Protection_biodiversity_and_ecosystems:	Ok
Protection_water_and_air:	Ok
Combatting_climate_change:	Ok
Manufacturer_company:	Beta
Address:	78, Beta street
Order_reference:	26487
Invoice_ID:	101711
Billing_address:	34, Gamma street
Gross_total:	\$5000
Company_VAT:	U12345678
Issue_date:	2022-05-12



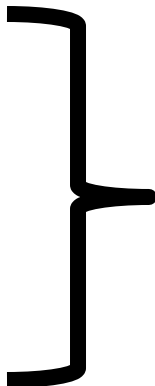
Focus



14548487, Carrier, International

Fundamental_workers_rights:	Ok
Human_rights:	Ok
Protection_biodiversity_and_ecosystems:	Ok
Protection_water_and_air:	Ok
Combatting_climate_change:	Ok

Customs or (14548487 and (Supplier and International))



Why?



Customs or (14548487 and (Supplier and International))



BRIE project

BRIE Blockchain Register for Import-Export

A blockchain-based solution to tracking and process optimisation in logistics



BRIE - Blockchain Register for Import Export - is a project co-funded by Cyber 4.0, according to the provisions of the Decree of the Minister of Economic Development No. 214 of 12.9.2017, within the framework of the interventions related to the National Plan Industry 4.0



moveax | Applied Innovation. Now.



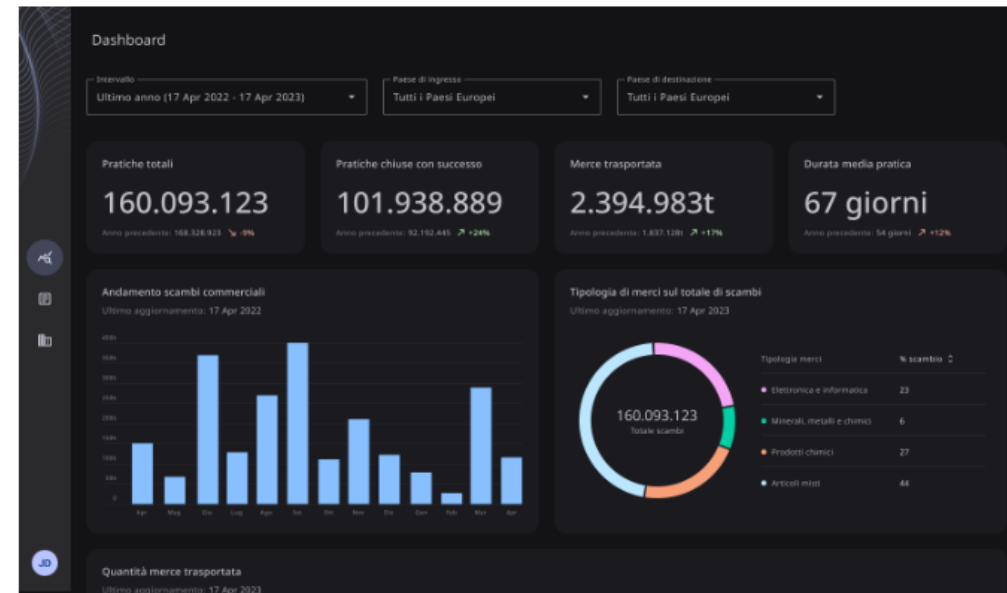
LUISS

BRIE

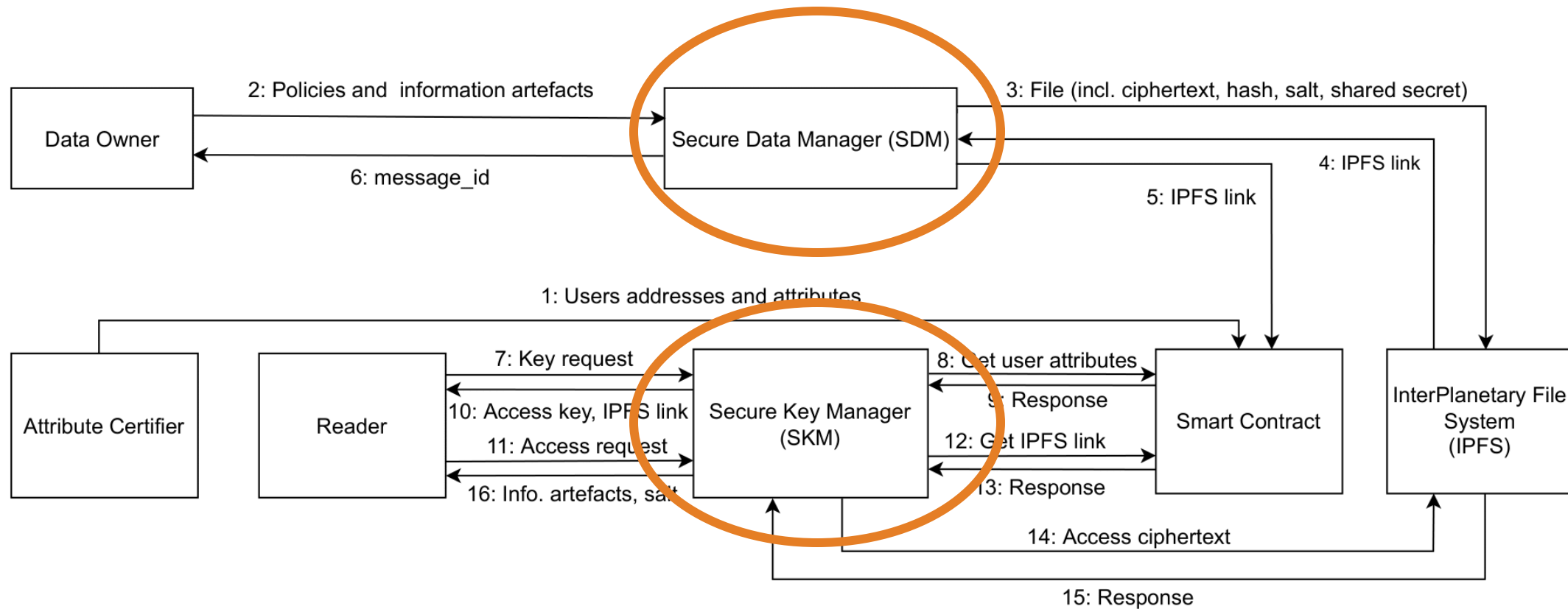
For info: info@moveax.it

Copyright 2023 All Rights Reserved

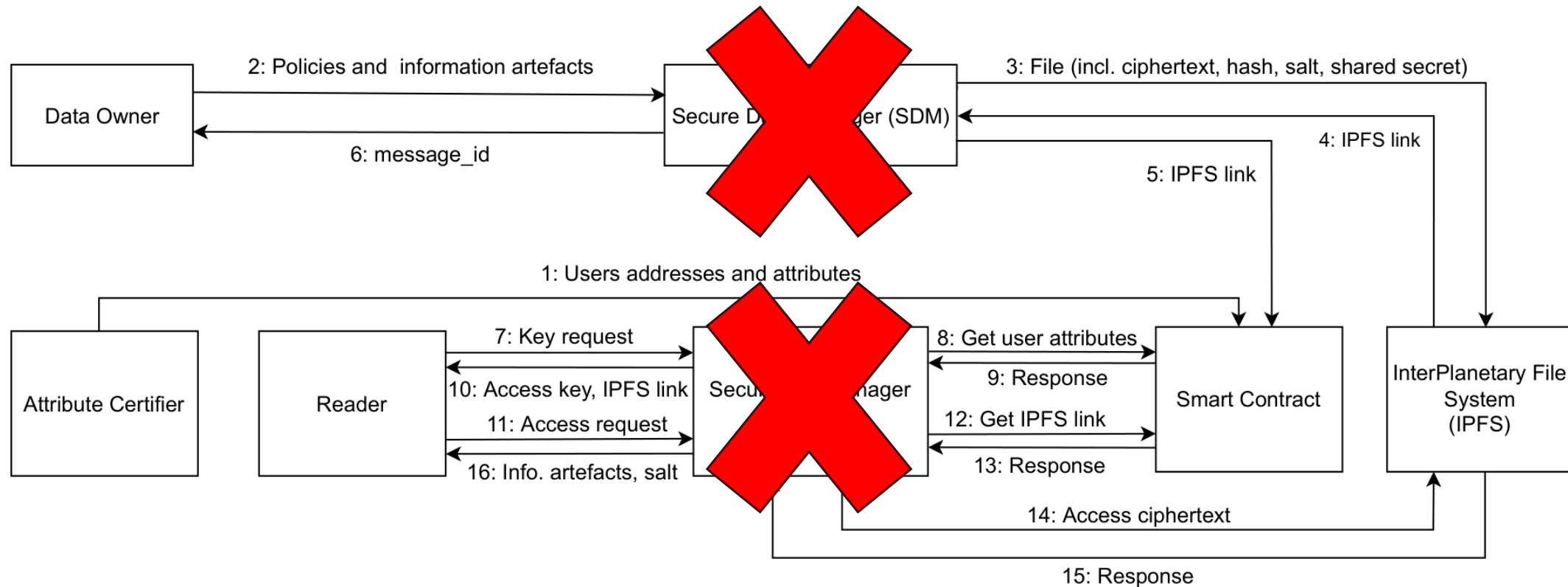
Website



CAKE architecture



CAKE architecture



MARTSIA

Multi-**A**uthority app**R**oach to **T**ransaction **S**ystem for **I**nteroperating
Applications

1. Edoardo Marangone, Claudio Di Ciccio, Daniele Friolo, Eugenio Nerio Nemmi, Daniele Venturi, and Ingo Weber. 2023. MARTSIA: Enabling Data Confidentiality for Blockchain-based Process Execution. In EDOC. Springer, 1–17. https://doi.org/10.1007/978-3-031-46587-1_4
2. Edoardo Marangone, Claudio Di Ciccio, Daniele Friolo, Eugenio Nerio Nemmi, Daniele Venturi, and Ingo Weber. 2023. Enabling Data Confidentiality with Public Blockchains. Submitted to ACM - TOPS. <https://arxiv.org/abs/2308.03791>

Ingredients

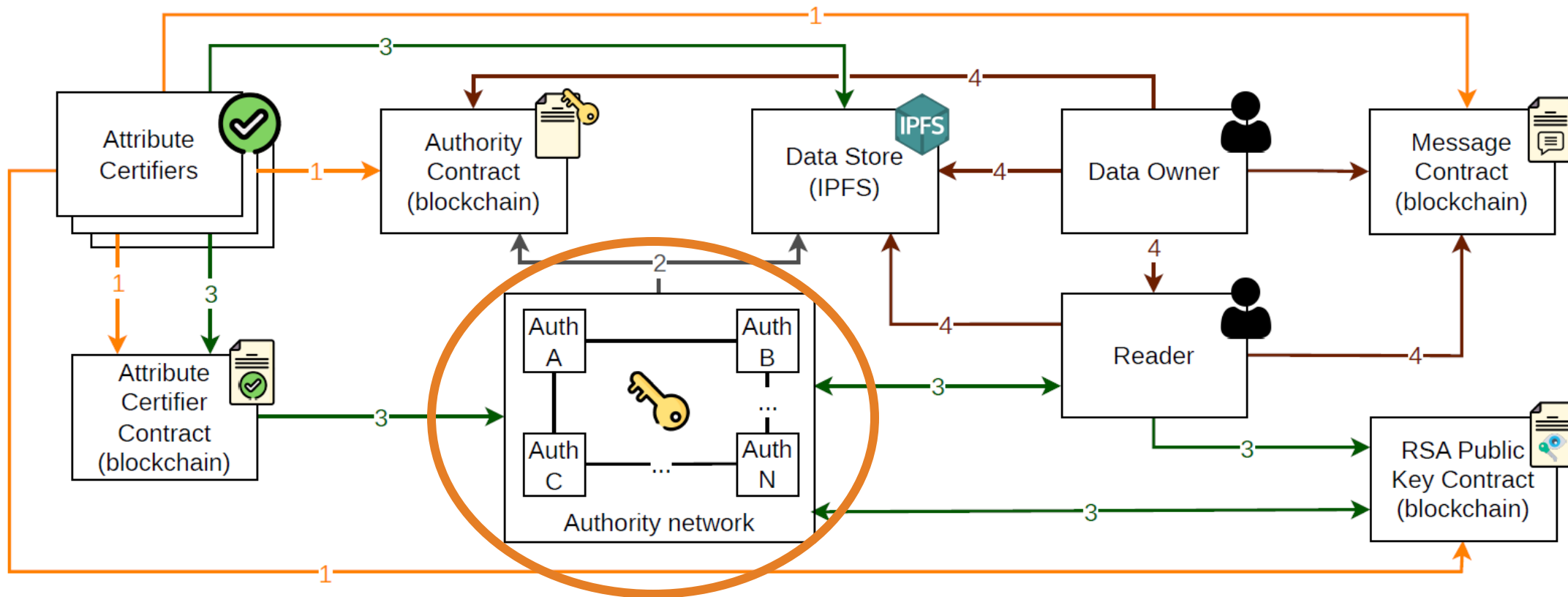
- Blockchains (EVM and Algorand)
- Smart Contracts
- InterPlanetary File System (IPFS)
- Multi-Authority Attribute-Based Encryption (MA-ABE):
Ciphertext-Policy MA-ABE (CP)

CP-MABE

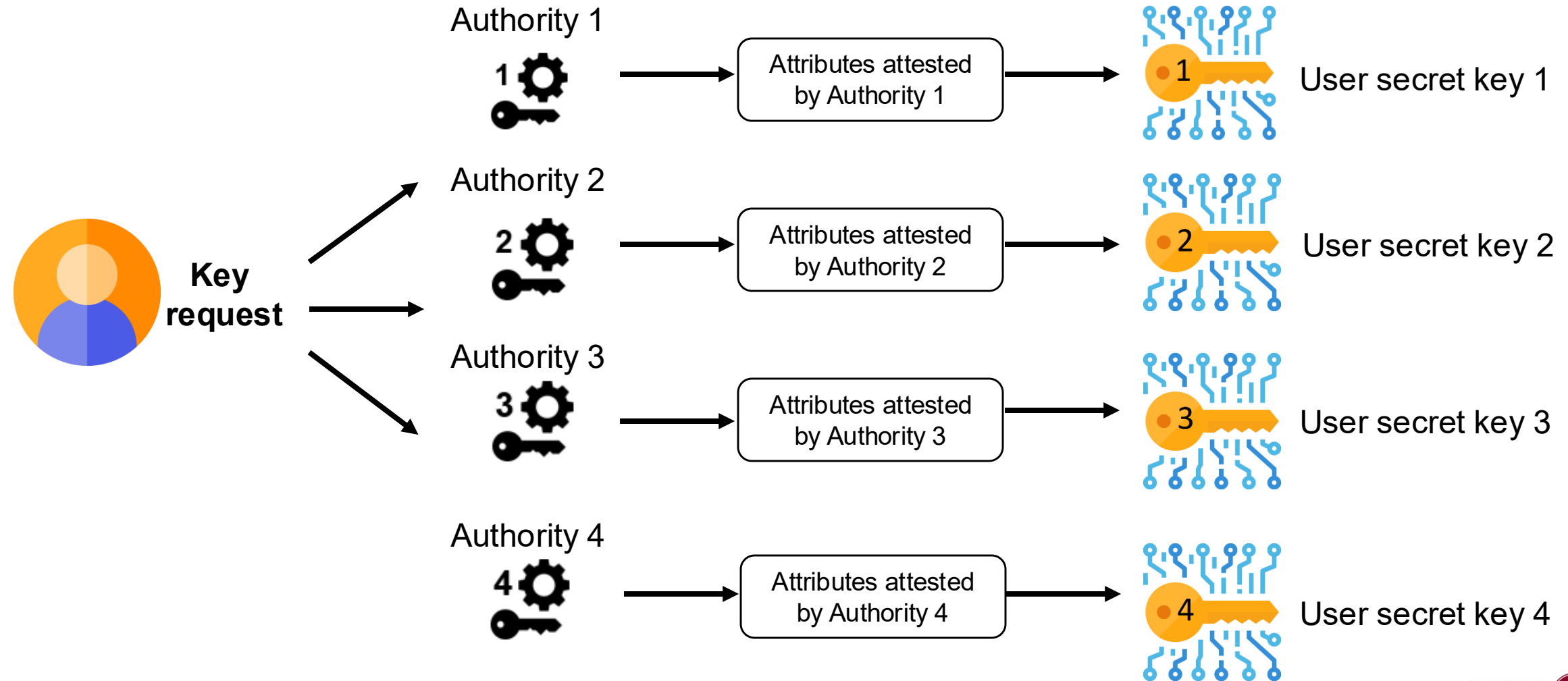
- Multi-Authority Attribute-Based Encryption (MA-ABE): type of public-key encryption
- Ciphertext-Policy MA-ABE (CP):
 - **Users** are associated with **attributes**
 - (propositional literals)
 - **Messages** are associated with **policies**
 - (propositional formulae on attributes)
- Attributes ex.:
43175279, Supplier, International, Manufacturer
- Policy ex.:
 $((43175279@AUTH1 \text{ and } 43175279@AUTH2 \text{ and } 43175279@AUTH3 \text{ and } 43175279@AUTH4) \\ \text{and } (Manufacturer@AUTH1 \text{ or } (Supplier@AUTH2 \text{ and } International@AUTH3)))$

The MARTSIA approach

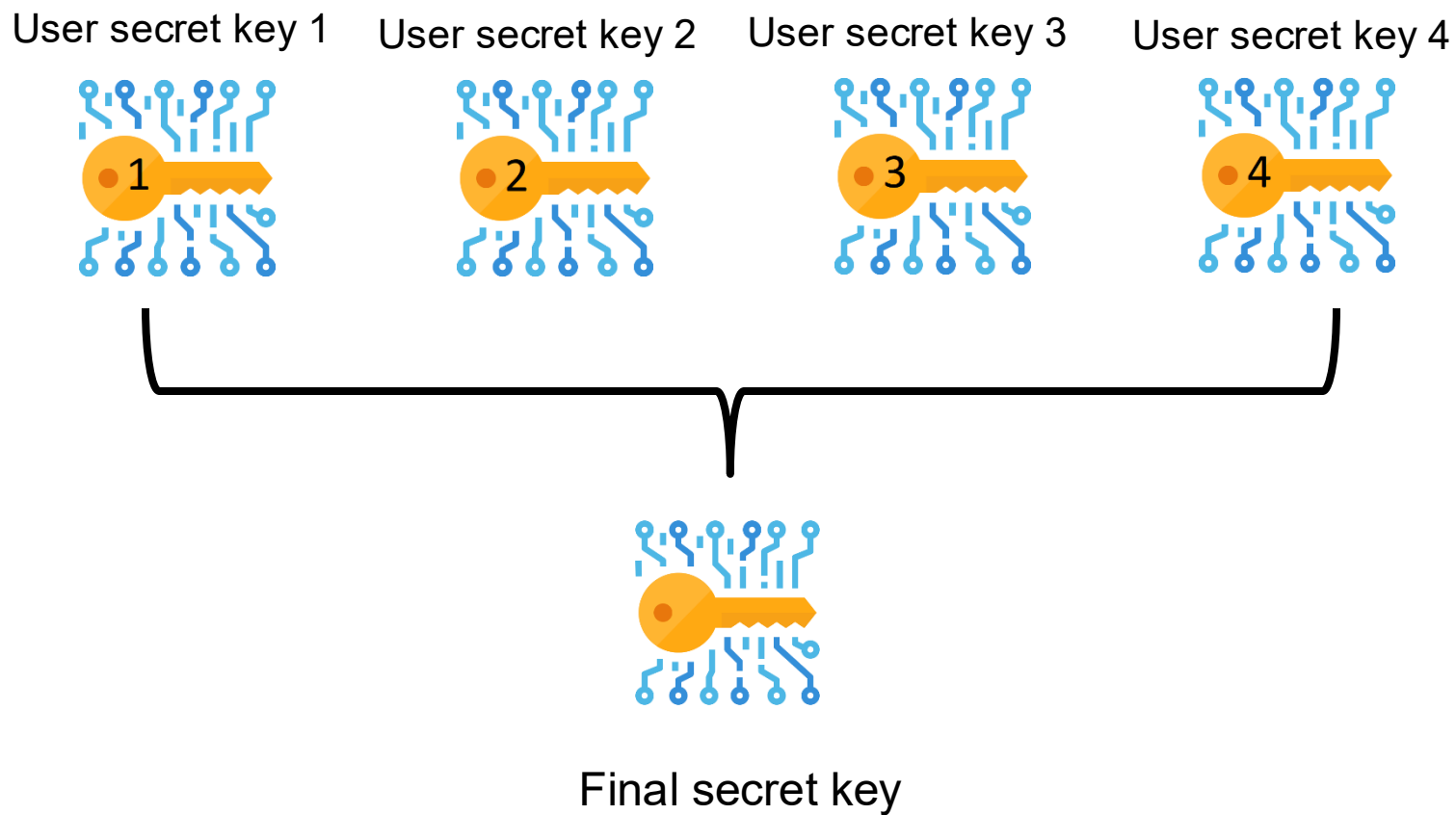
MARTSIA approach



Reader



Reader



Focus



43175279@1@2, International@3, Carrier@4

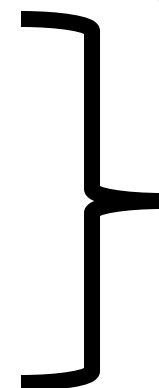


x4

Fundamental_workers_rights:	Ok
Human_rights:	Ok
Protection_biodiversity_and_ecosystems:	Ok
Protection_water_and_air:	Ok
Combatting_climate_change:	Ok



Customs@A or
(43175279@2+ and
(International@1+ and
Supplier@1+))



Why?

Customs@A or (43175279@2+ and (International@1+ and Supplier@1+))



Health-e-Data project

Health-e-Data: al servizio dell'innovazione sanitaria

Perchè Health-e-Data

L'accesso e l'utilizzo dei dati sanitari costituiscono passaggi essenziali per abilitare lo sviluppo di **soluzioni digitali innovative in ambito medicale**. Gli algoritmi di intelligenza artificiale hanno bisogno di **grandi quantità di dati** per essere addestrati e validati.

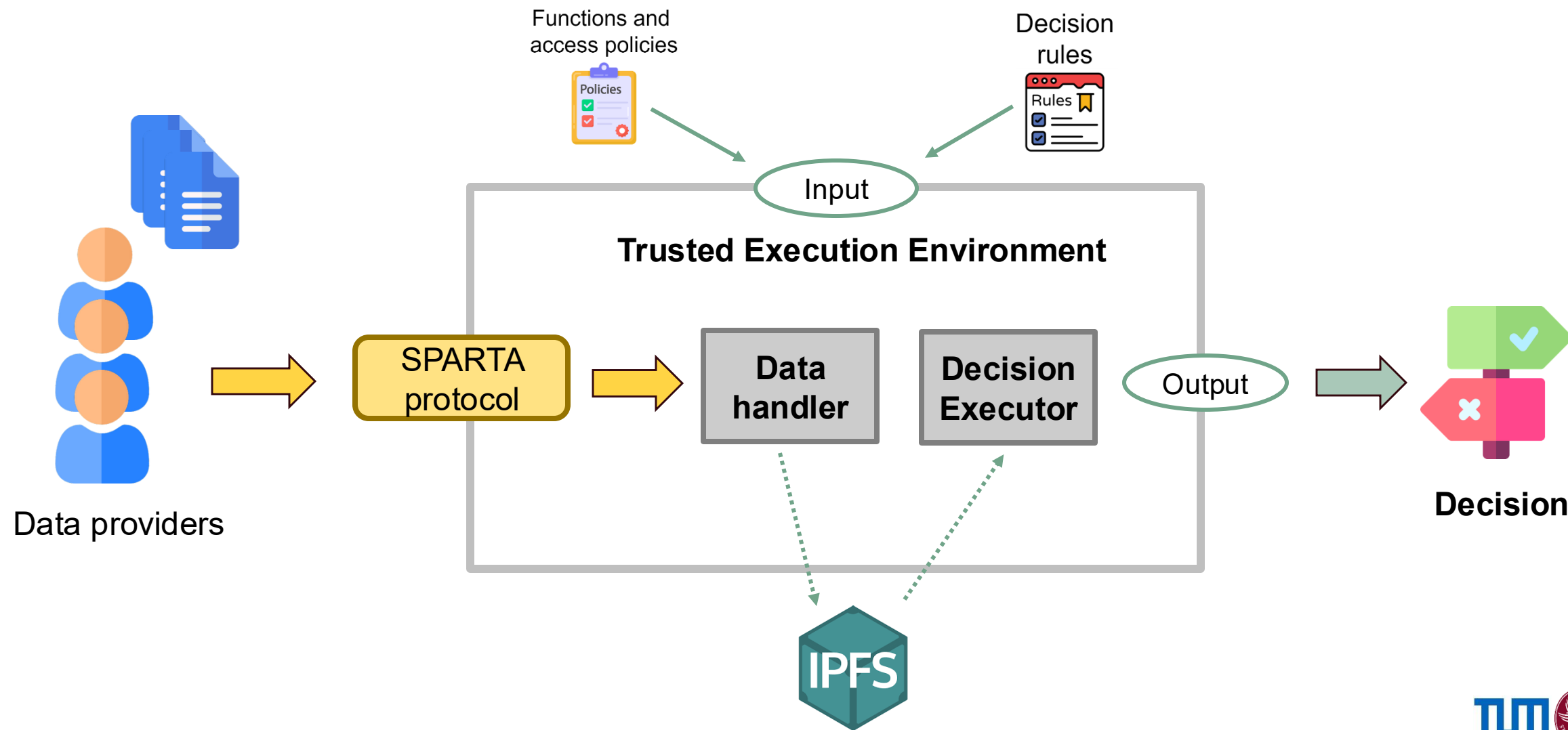
Health-e-Data è un progetto di innovazione che si propone di sviluppare un sistema innovativo basato su **blockchain** e **intelligenza artificiale** per facilitare l'accesso sicuro e l'uso dei dati, nel pieno rispetto della privacy, consentendo ad ospedali e cittadini di mantenere pieno controllo sui loro dati.

Website



Current work

Decision-support system with TEEs



Papers:

CAKE

Paper



GitHub



MARTSIA

Paper



GitHub



Acknowledgement : Papers about provenance, processing, traceability and security of data exchange and logging within business processes (areas of interest for the PINPOINT project – in particular for the work package 1, Transparent end-to-end data extraction and transformation. <https://pinpoint.unibz.it/>)