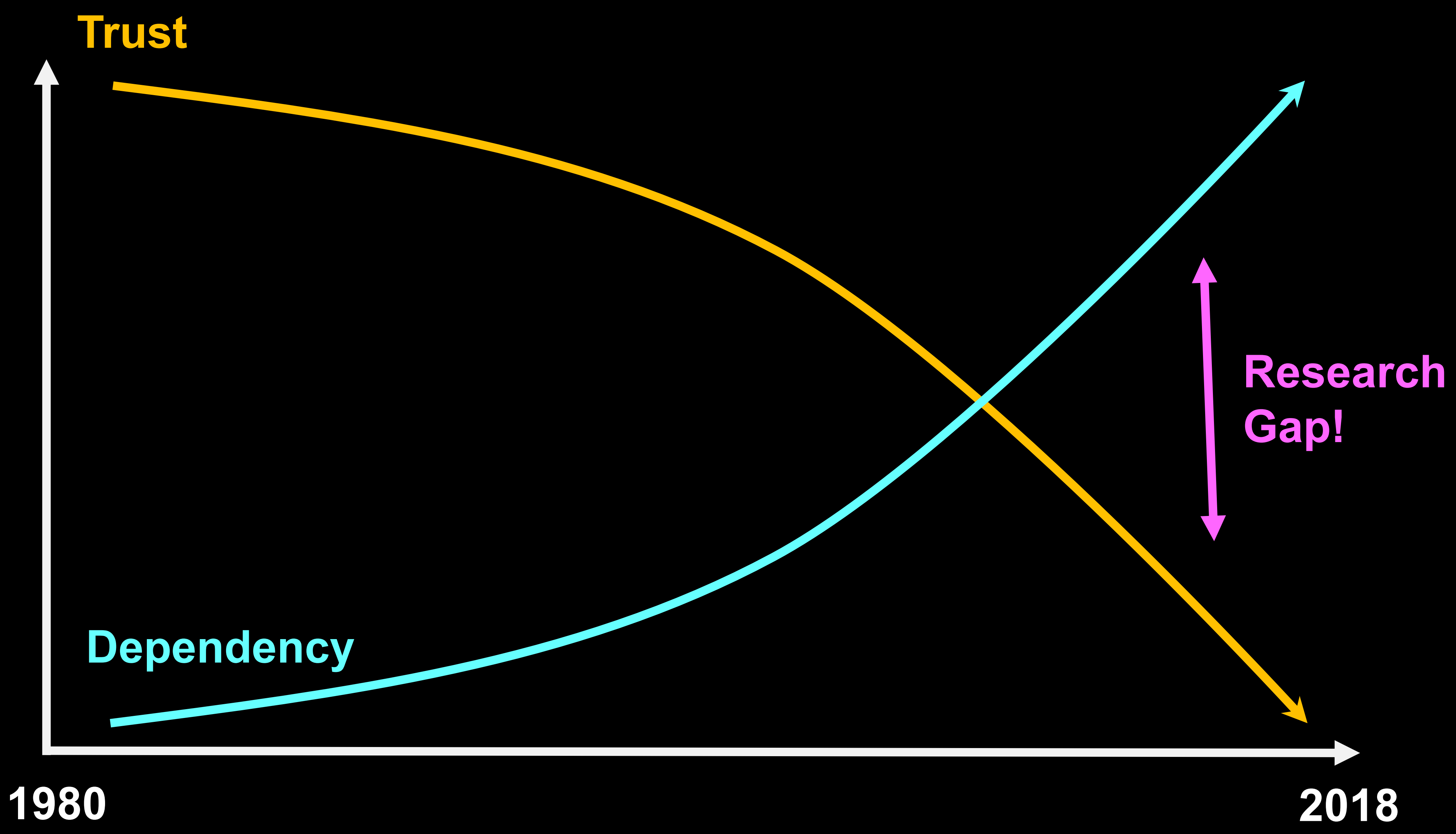
Digital Data Markets:
Trusted Data Processing in Untrusted Environments

Cees de Laat

Systems and Networking Laboratory
University of Amsterdam

Fading Trust in Internet



Harvard Business Review

☰ Harvard Business Review | Subscribe | Sign In | Register

ECONOMY

Managing Our Hub Economy

by Marco Iansiti and Karim R. Lakhani

FROM THE SEPTEMBER–OCTOBER 2017 ISSUE

WHAT TO READ NEXT

The IT Transformation Health Care Needs

SUMMARY | SAVE | SHARE | 3 COMMENT | TEXT SIZE | PRINT | $8.95 BUY COPIES

THOMAS M. SCHEER/EYEEM/GETTY IMAGES

I. The Problem

The global economy is coalescing around a few digital superpowers. We see unmistakable evidence that a winner-take-all world is emerging in which a small number of “hub firms”—including Alibaba, Alphabet/Google, Amazon, Apple, Baidu, Facebook, Microsoft, and Tencent—occupy central positions. While creating real value for users, these companies are also capturing a disproportionate and expanding share of the value, and that’s shaping our collective economic future. The very same technologies that promised to democratize business are now threatening to make it more monopolistic.

HARVARD BUSINESS PUBLISHING

Data value creation monopolies

→

Create an equal playing field

→

Sound Market principles

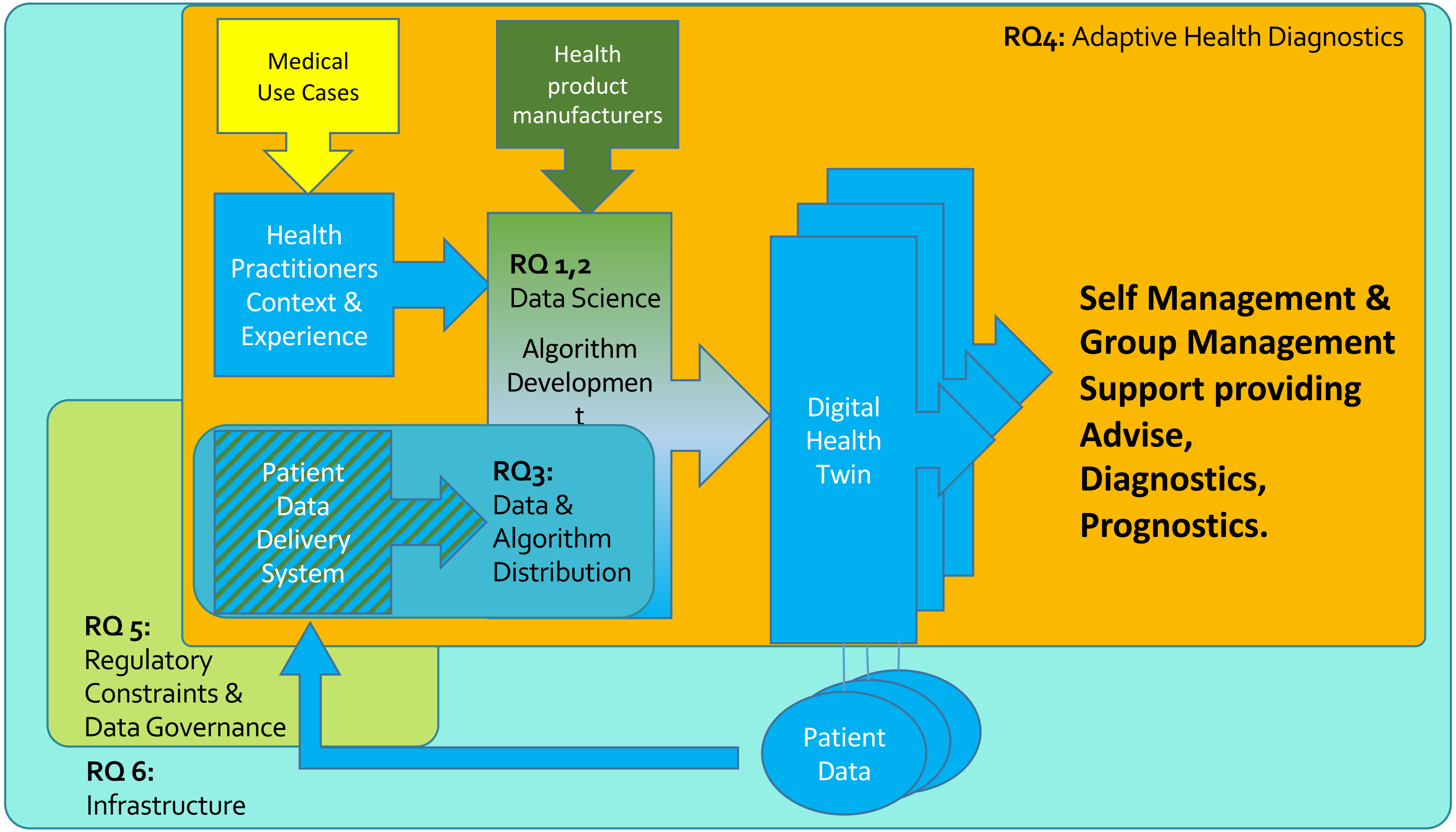
https://hbr.org/2017/09/managing-our-hub-economy

Main problem statement

- Organizations that normally compete have to bring data together to achieve a common goal!
- The shared data may be used for that goal but not for any other!
- Data may have to be processed in untrusted data centers.
  - How to enforce that using modern Cyber Infrastructure?
  - How to organize such alliances?
  - How to translate from strategic via tactical to operational level?
  - What are the different fundamental data infrastructure models to consider?

Health use case

Enabling Personal Interventions



Big Data Sharing use cases placed in airline context

Global Scale

National Scale

City / regional Scale

Campus / Enterprise Scale

Aircraft Component Health Monitoring (Big) Data
NWO **CIMPLO project**
4.5 FTE

Cargo Logistics Data
(C1) DL4LD
(C2) Secure scalable policy-enforced distributed data Processing
(using blockchain)

NLIP iShare project

iSHARE
powered by NLIP

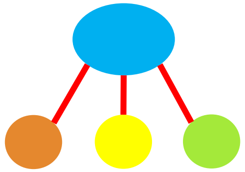
Cybersecurity Big Data
NWO COMMIT/
SARNET project
3.5 FTE

RESEARCH WORKING ALONGSIDE IT INDUSTRY

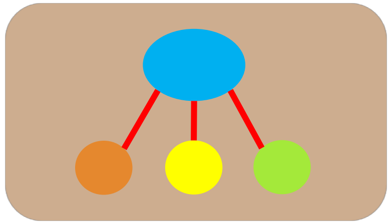
NETWORK RESEARCH INFRASTRUCTURES

COMMERCIAL DATACENTER INFRASTRUCTURE AS NEUTRAL GROUND

Data Sharing Infrastructure Model Research using Future Internet capabilites



Research collaboration

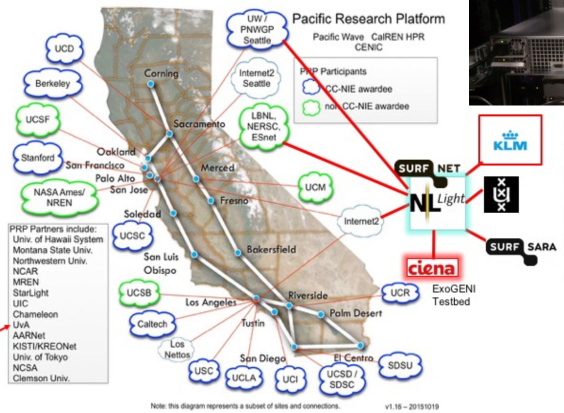


Goal: How to create a Digital Marketplace Ecosystem

PACIFIC RESEARCH PLATFORM

prp.ucsd.edu

As foundation of the National Research Platform

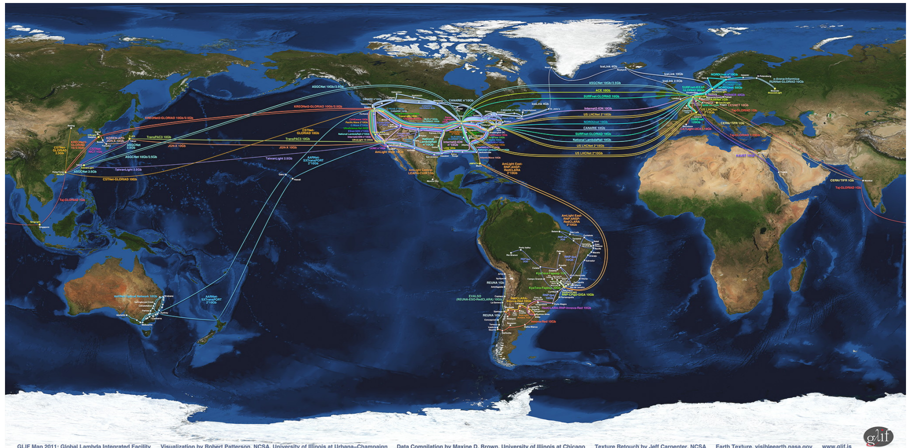


Data Transfer Node at KLM fieldlab with 100 gb/s link to enable SDMP research thanks to UvA, SURFnet and Ciena

AM3 and AM4 Datacenters Science Park Amsterdam

SV10 Datacenter Silicon Valley

Gobal Lambda Integrated Facility ➔



ANCE KLM

Approach

- Strategic:
  - Translate legislation into machine readable policy
  - Define data use policy
  - Trust evaluation models & metrics
- Tactical:
  - Map app given rules & policy & data and resources
  - Bring computing and data to (un)trusted third party
  - Resilience
- Operational:
  - TPM & Encryption schemes to protect & sign
  - Policy evaluation & docker implementations
  - Use VM and SDI/SDN technology to enforce
  - Block chain to record what happened (after the fact!)

Data Processing models

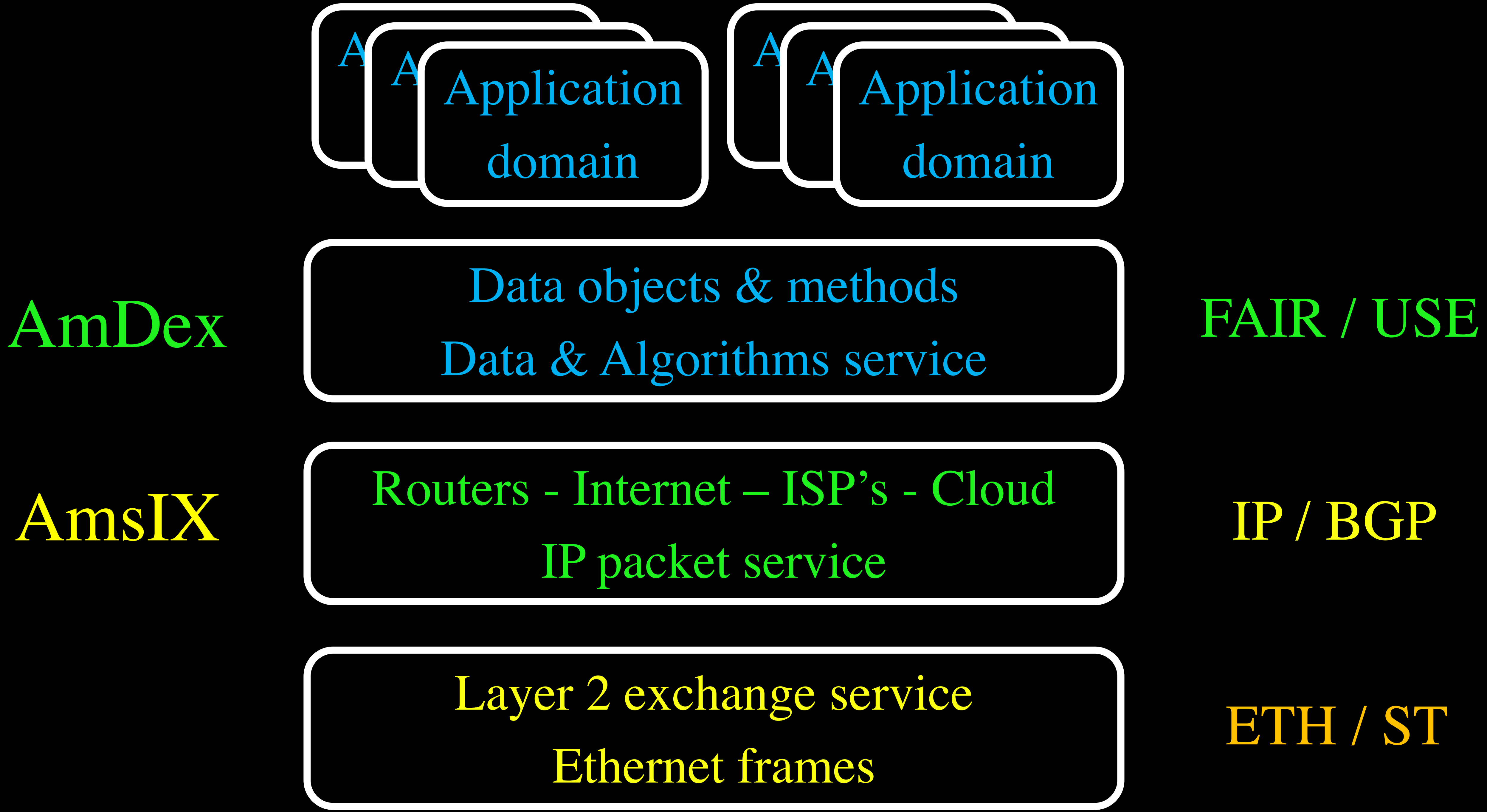
- Bring data to computing
- Bring computing to data
- Bring computing and data to (un)trusted third party
- A mix of all of the above
- Block chain to record what happened
- Block chain for data integrity
- Bring the owner of Data in control!
- Data owner policy + enforcement technology

IETF: Common Open Policy Service (COPS)

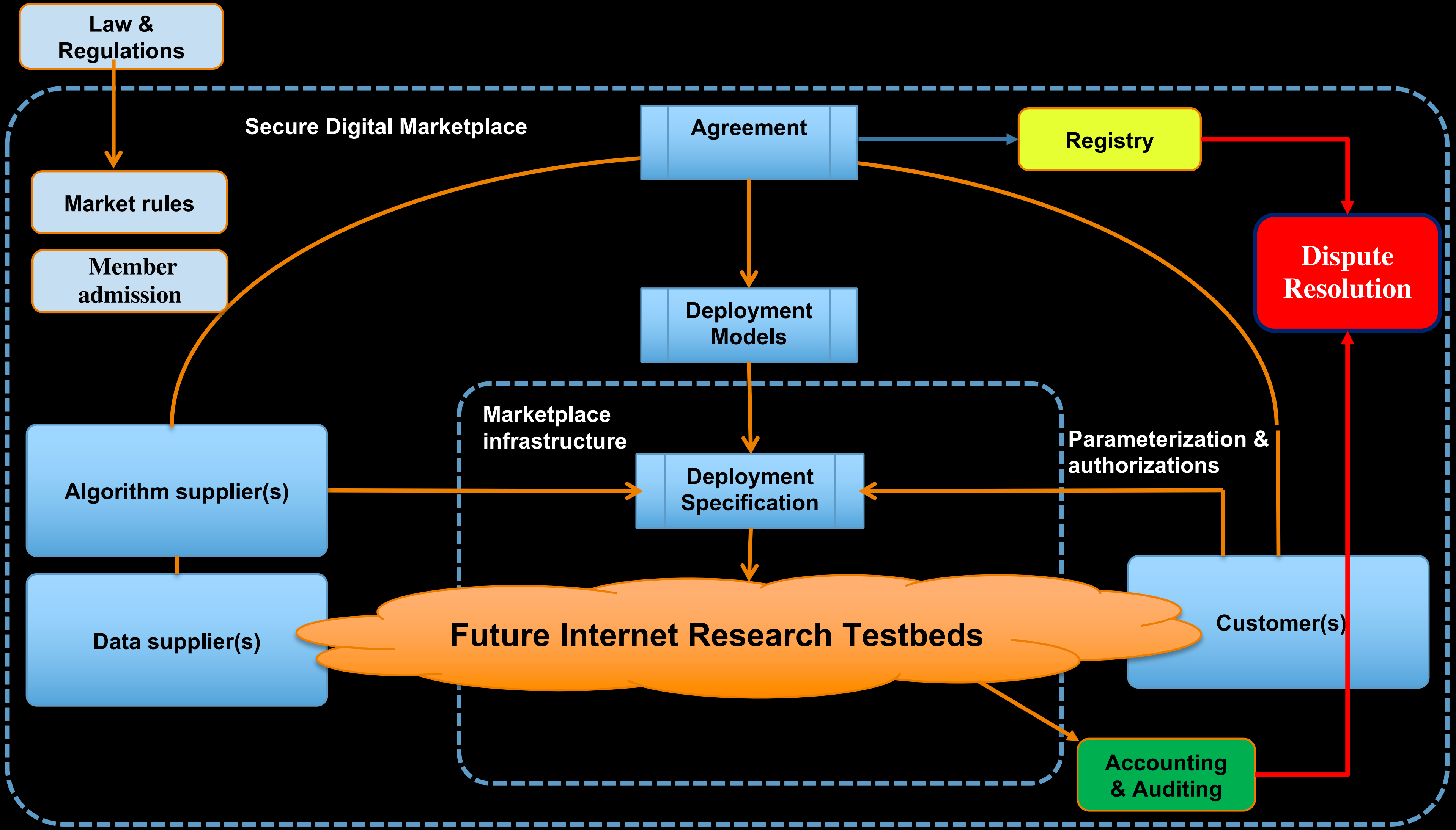
- Rfc 2748, 2753, 4261

```
 ________________                     ____________________
|                |                   |                    |
|  Network Node  |  Policy Server    |    Network Node    |
|    _____       |      _____        |  _____      _____  |
|   |     |      |     |     |       | |     |    |     | |
|   | PEP |<-----|---->| PDP |       | | PEP |<-->| PDP | |
|   |_____|      |     |_____|       | |_____|    |_____| |
|     ^          |                   |                    |
|     |    _____ |                   |____________________|
|     \-->|     ||
|         | LPDP||
|         |_____||
|                |
|________________|
```

☺

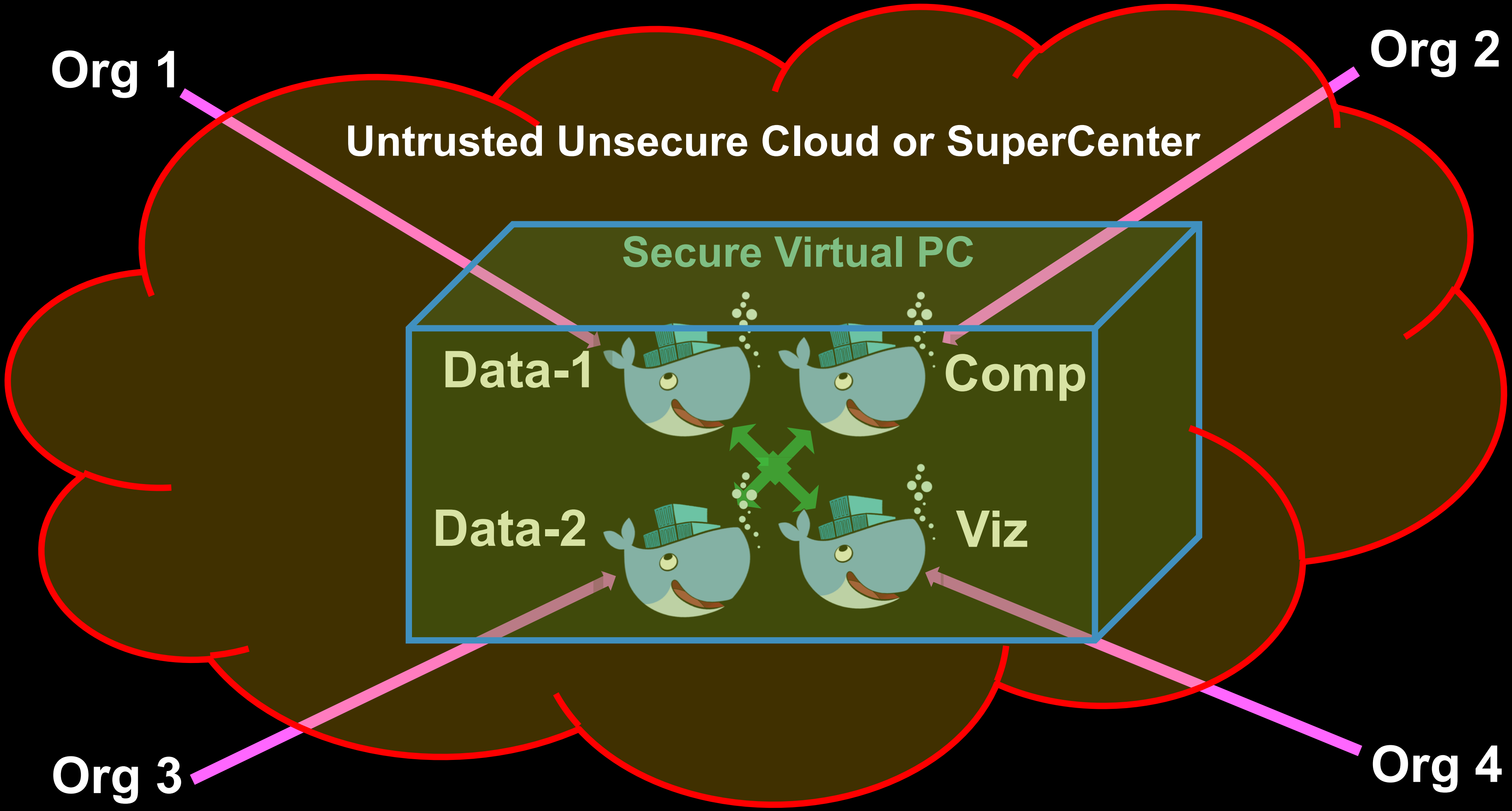

Application domain
Application domain
AmDex
Data objects & methods
Data & Algorithms service
FAIR / USE
AmsIX
Routers - Internet – ISP’s - Cloud
IP packet service
IP / BGP
Layer 2 exchange service
Ethernet frames
ETH / ST

Secure Digital Market Place Research

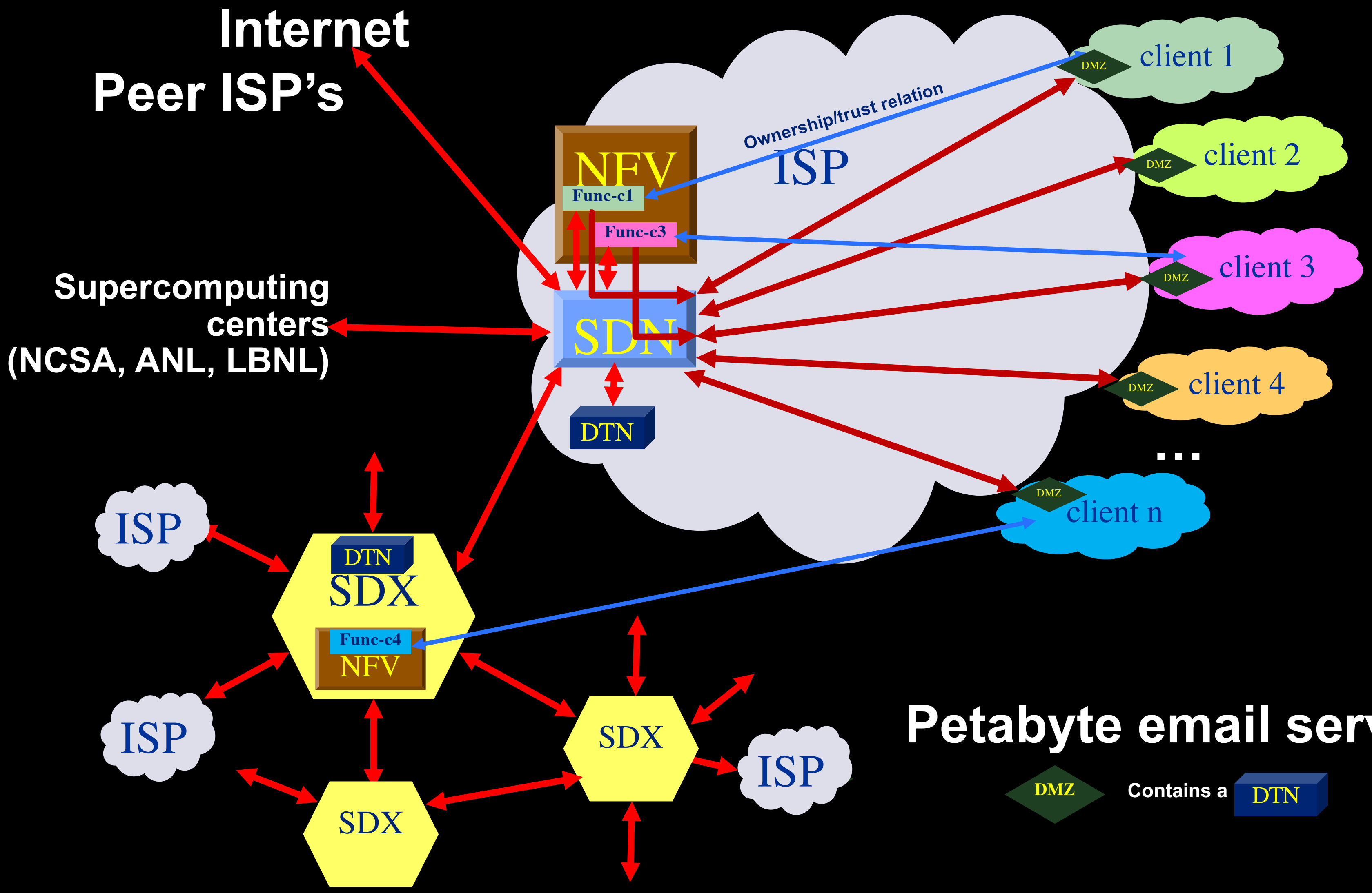


Secure Policy Enforced Data Processing

- Bringing data and processing software from competing organisations together for common goal
- Docker with encryption, policy engine, certs/keys, blockchain and secure networking
- Data Docker (virtual encryped hard drive)
- Compute Docker (protected application, signed algorithms)
- Visualization Docker (to visualize output)



Networks of ScienceDMZ's & SDX's



Petabyte email service ☺

DMZ Contains a DTN

What have we been doing?

- Studying and defining draft Policy
- Working out model & defining Archetypes
- Implementing a proof of concept using several distributed DTN's and dockers on kubernetes.
- Working on a demo for SC18 in Dallas TX, 11-16 Nov.
- Tactical operation of Digital Data Markets
- Optimization of degrees of freedom == value

SC16 Demo

DockerMon Sending docker containers with search algorithms to databases all over the world.

http://sc.delaat.net/sc16/index.html#5

Container-based remote data processing

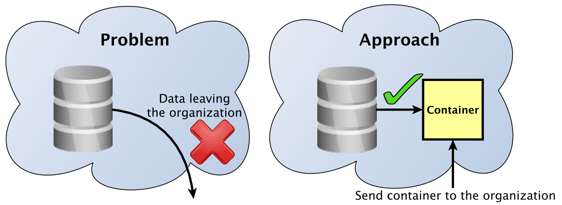
Universiteit van Amsterdam

Łukasz Makowski, Daniel Romão, Cees de Laat, Paola Grosso
System and Networking Research Group, University of Amsterdam

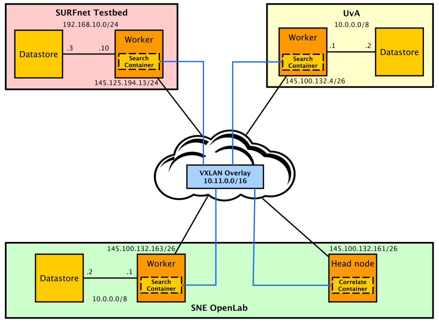
System and Network Engineering

Problem Description

- Scientific datasets are usually made publicly available
  ….but data cannot always leave the organization premises
- On-site data processing can be challenging because of incompatibility of systems or lack of manpower
- Can a container-based system perform remote on-site data processing efficiently?
- What are the networking issues to solve?



Underlay and Overlay



Main features:

- Networked containers
- VXLAN overlay
- Containers that perform data retrieval and computation
- Containers built on-demand
- On-site data processing
- Distributed data source
- Multiple sites with datasets

The Game

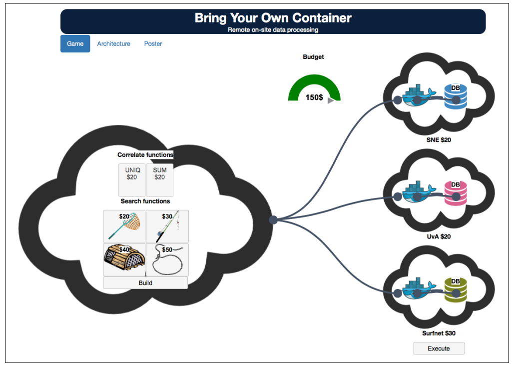
Our SC16 demo is a gamification of the remote dataset processing architecture.

How many different animal species can you find? You have a fixed budget and each function and processing will cost you money!

In our game you will:

- Select a correlate function to combine the results of the different sites.
- Pick different search functions, represented as tools, to find animals in the remote datasets.
- Build containers with the search and correlate functions.
- Execute the containers on the sites of your choice.

Will you have the best score?



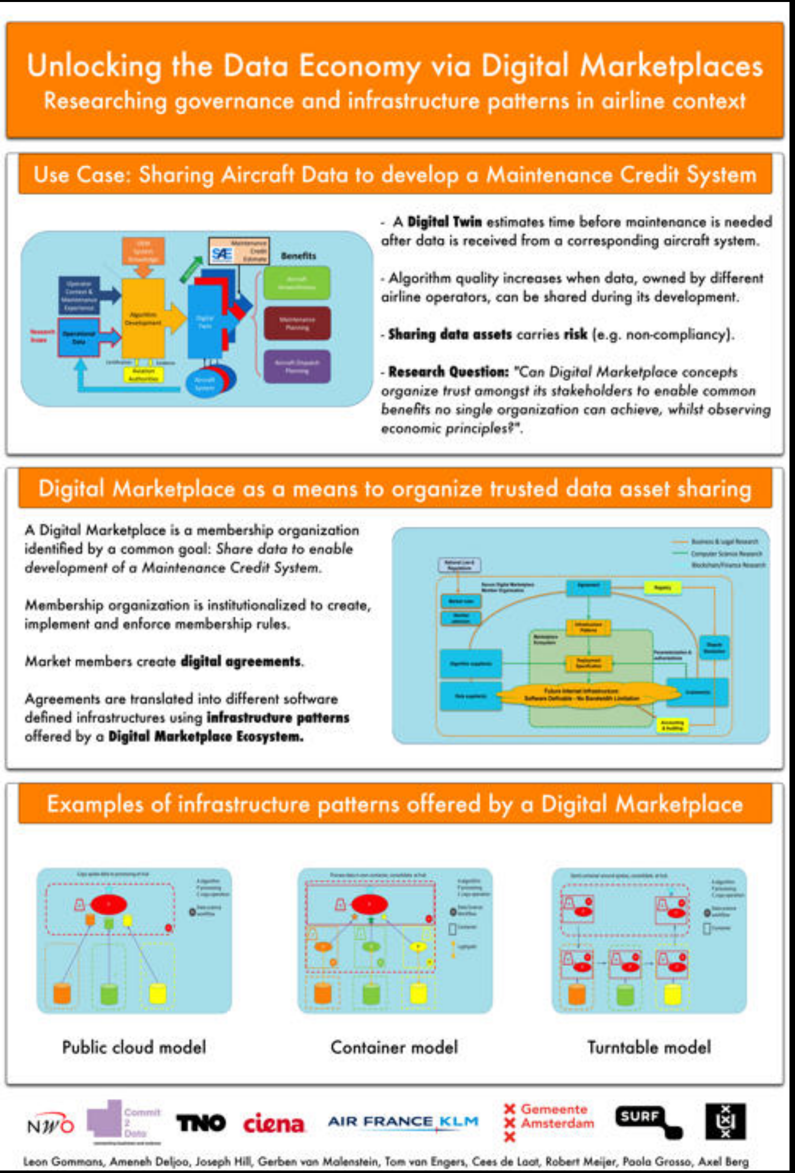
More information:

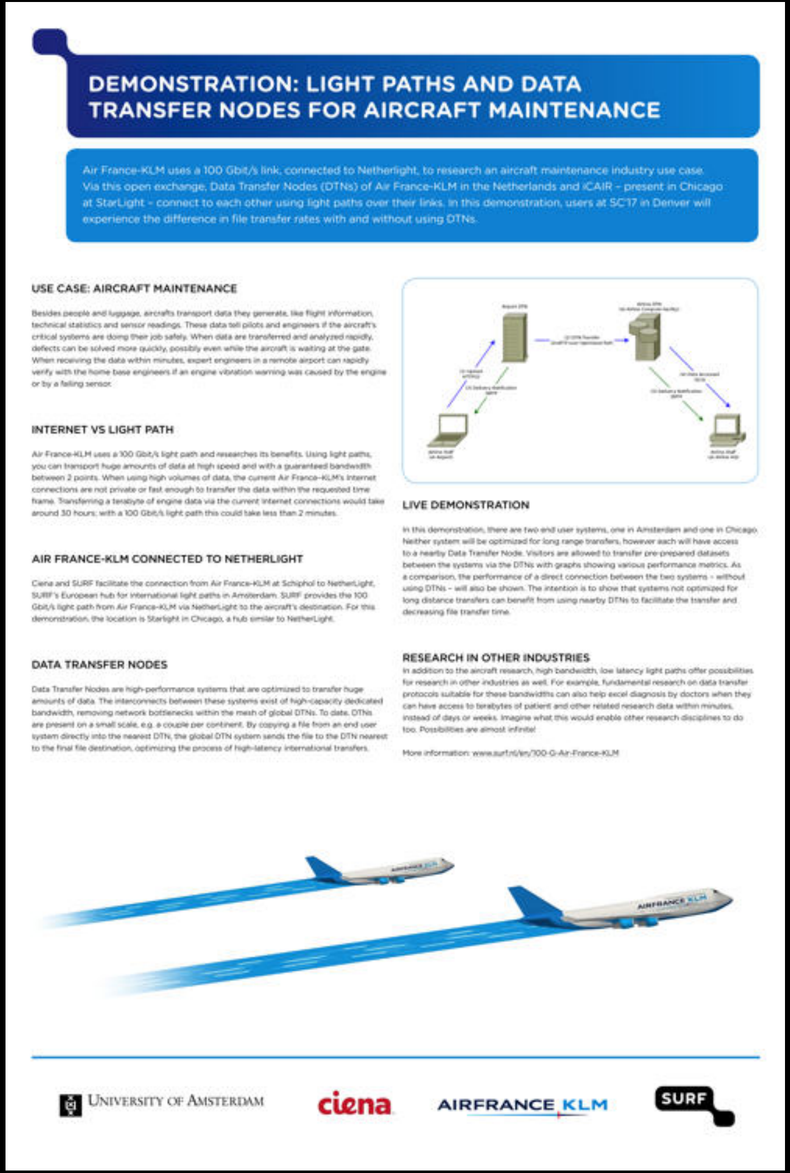
- http://byoc.lab.uvalight.net/info
- http://sne.science.uva.nl/sne/gigaport3
- http://delaat.net/sc

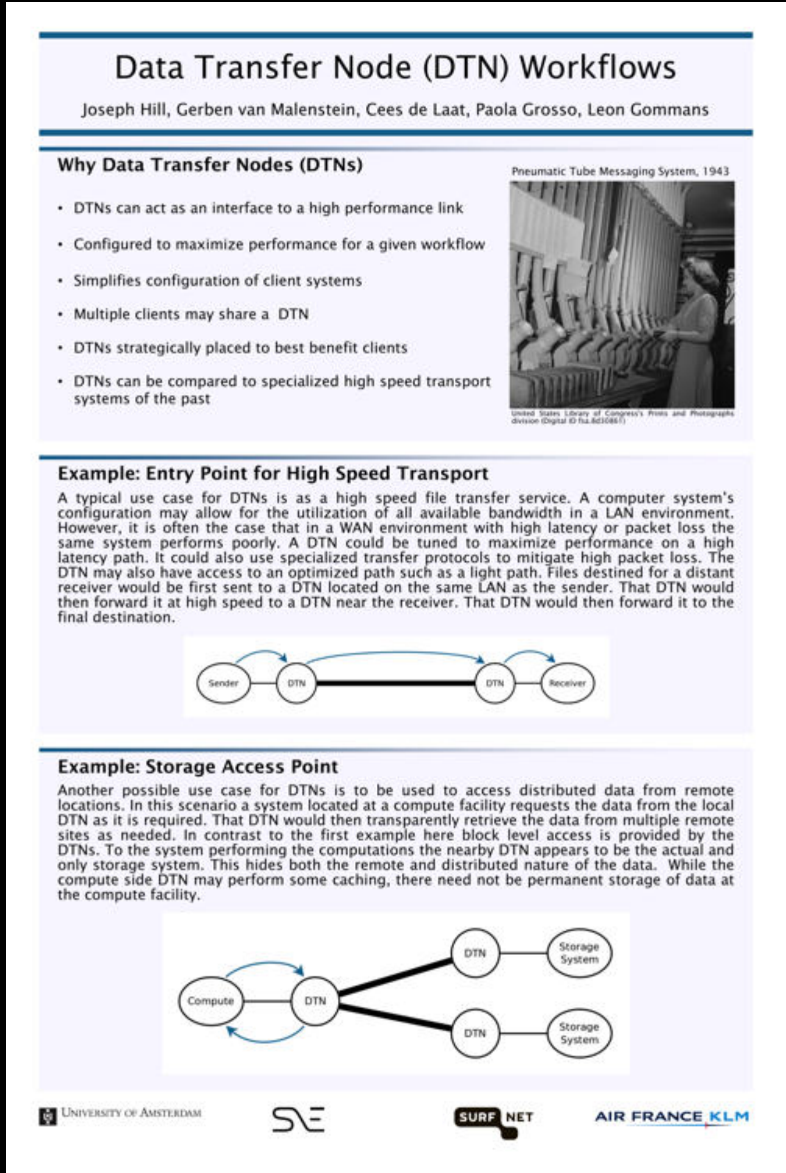
SURF NET

SC17 Posters and proof of concepts & demo’s

http://sc.delaat.net/sc17





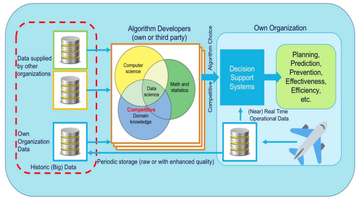


SC18 – Dallas TX

Training AI/ML models using Digital Data Marketplaces

Creating value and competition by enabling access to additional big data owned by multiple organizations in a trusted, fair and economic way

The more data - the better: an aircraft maintenance use-case



- AI/ML algorithm based Decision Support Systems create business value by supporting real-time complex decision taking such as **predicting the need for aircraft maintenance**.

- Algorithm quality increases with the availability of aircraft data.

- Multiple airlines operate the same type of aircraft.

- **Research Question:** *"How can AI/ML algorithm developers be enabled to access additional data from multiple airlines?"*

- **Approach:** *Applying Digital Data Marketplace concepts to facilitate trusted big data sharing for a particular purpose.*

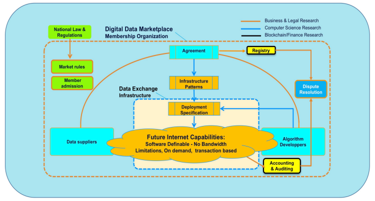
Digital Data Marketplace enabling data sharing and competition

A **Digital Data Marketplace** is a membership organization supporting a common goal: e.g. *enable data sharing to increase value and competitiveness of AI/ML algorithms.*

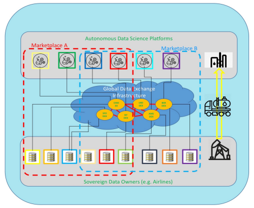
Membership organization is institutionalized to create, implement and enforce membership rules organizing **trust**.

Market members arrange **digital agreements** to exchange data for a **particular purpose** under specific conditions.

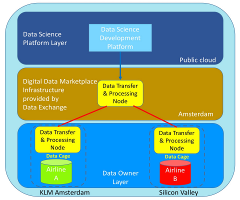
Agreements subsequently drive data science transactions creating processing infrastructures using infrastructure patterns offered by a Data Exchange as **Exchange Patterns**.



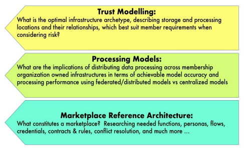
Researching Exchange Patterns to support Digital Data Marketplaces



Data Exchange Model



Research Infrastructure



Research Elements

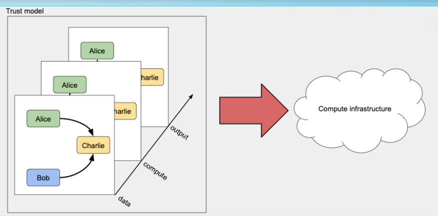
Leon Gommans, Anne Savelkoul, Wouter Kalfsbeek, Dirk van den Herik, David Langerveld, Erik IJzermans, Floris Freeman, Brend Dikkers, Cees de Laat, Tom van Engers, Wouter Los, Paola Grosso, Joseph Hill, Reggie Cushing, Giovanni Sileno, Lu Zhang, Ameneh Deljoo, Thomas Baeck, Willem Koeman, Laurie Strom, Axel Berg, Gerben van Malenstein, Kaladhar Voruganti, Patricia Florissi

Dataharbours: computing archetypes for digital marketplaces

Reginald Cushing, Lu Zhang, Paola Grosso, Tim van Zalingen, Joseph Hill, Leon Gommans, Cees de Laat, Vijaay Doraiswamy, Purvish Purohit, Kaladhar Voruganti, Craig Waldrop, Rodney Wilson, Marc Lyonnais

The problem

How can competing parties share compute and data? The architecture of a digital marketplace is an active research field and has many components to it. Here we investigate a federated computing platform which is molded into different **archetypes** based on **trust** relationships between organizations.



The components

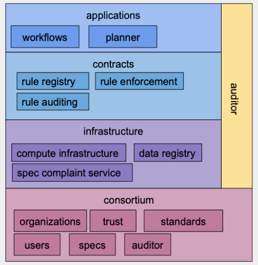
Consortium: is an initial document which brings together organizations that wish to collaborate. It defines static information such as keys to identify parties.

Infrastructure: A single domain organization infrastructure that securely hosts data, compute containers and, optionally, compute infrastructure. We dub this infrastructure a **data harbour**. A harbour implements a set of protocols that allows it to interact with other harbours.

Contracts: Are a set of rules that are shared amongst participating harbours which describe how objects (data, compute) can be traded between harbours and who can process data. In its simplest form is a 7-tuple which binds a user, data object, compute container, contract, consortium, harbour, and expiry date.

An application: Is a distributed pipeline which can make use of several contracts. The combination of application and contract defines the archetype of the computation i.e. how data and compute are moved to effect computation.

Auditor: A trusted entity that collects audit trails for use in litigation of policy violations.

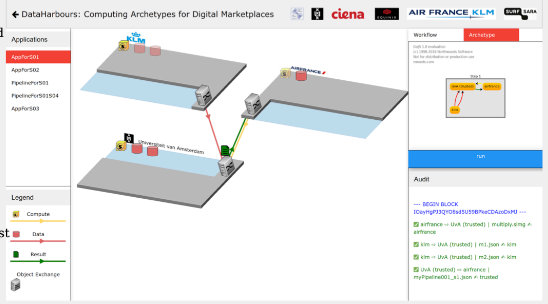


In action

Federated computing on 3 distributed data harbours. Here we illustrate one archetype where KLM and Airfrance do not trust each other and employ a trusted 3rd party to send the data and compute for processing.

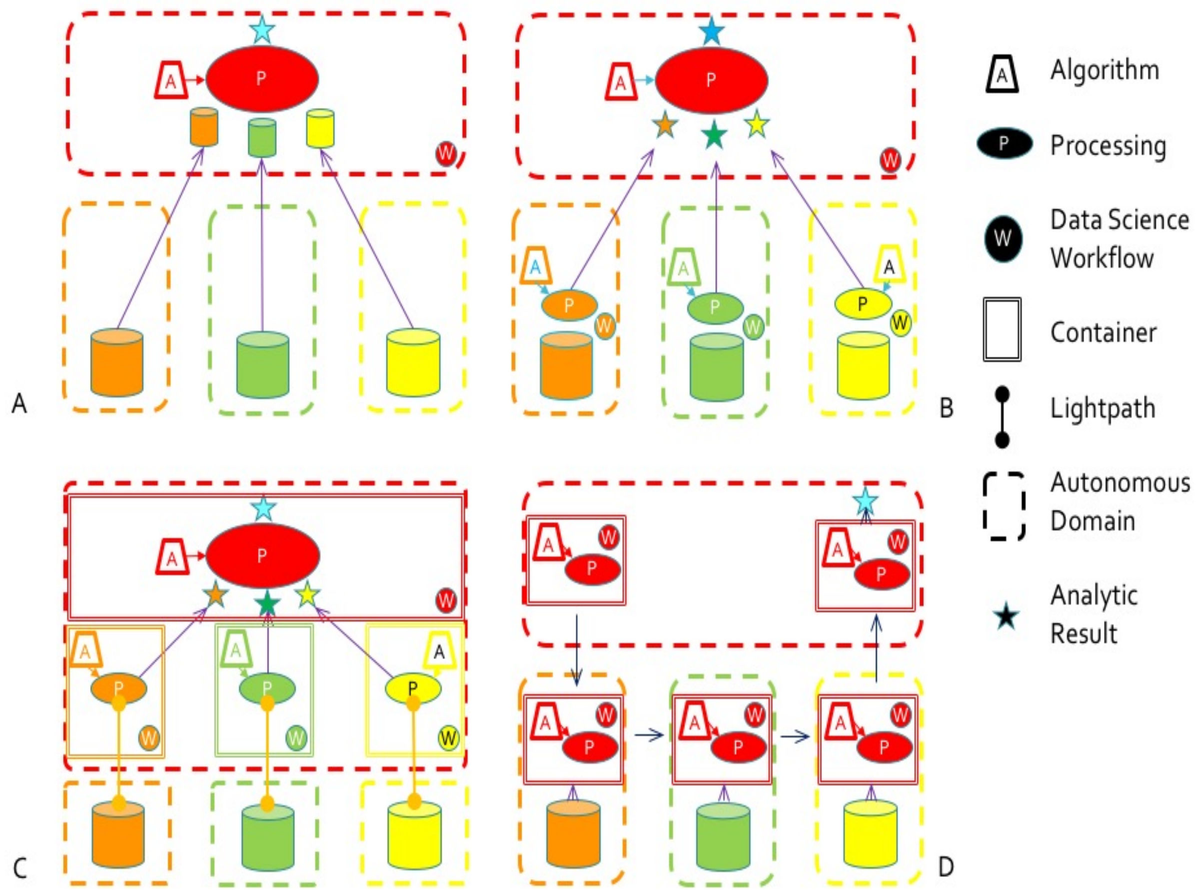
For the scenario to succeed the different harbours need to effect several transactions which are governed by contractual rules.

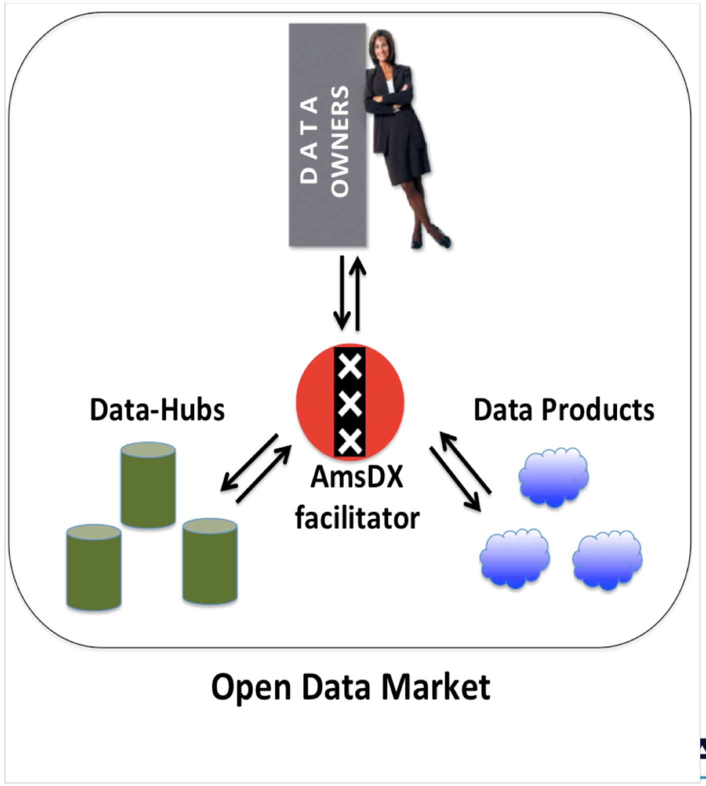
The transaction **protocol** involves first identifying both parties are who they say they are through pub/priv key challenges and secondly, that at least a **contract** rule is matched to allow the transaction. Important steps of the transactions are **audit** logged i.e. signed and published to and audit log collector.



INFRASTRUCTURE PATTERN EXAMPLES

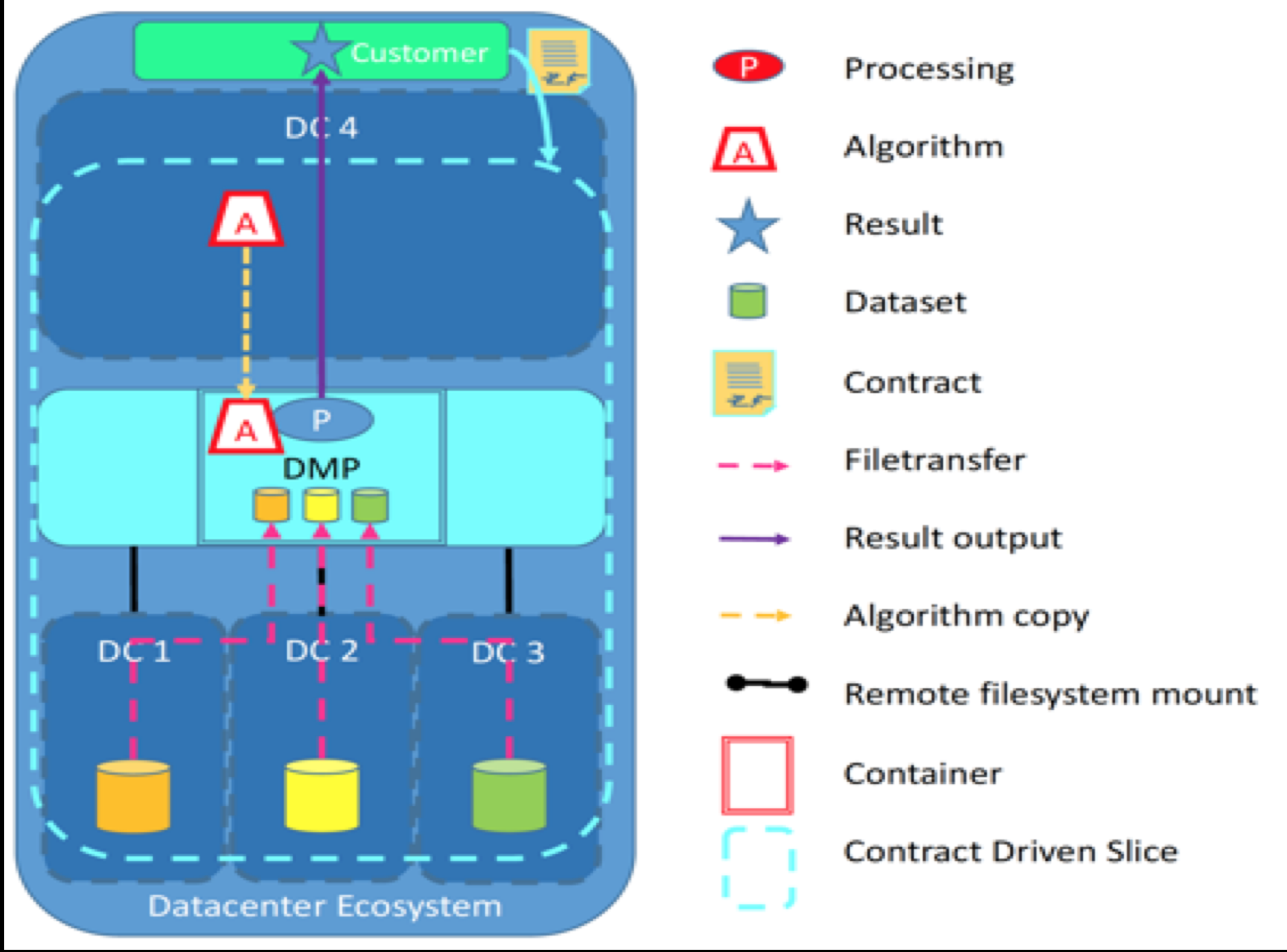
OFFERED BY A DATA EXCHANGE TO MARKETPLACES TO CHOOSE FROM





ANCE KLM

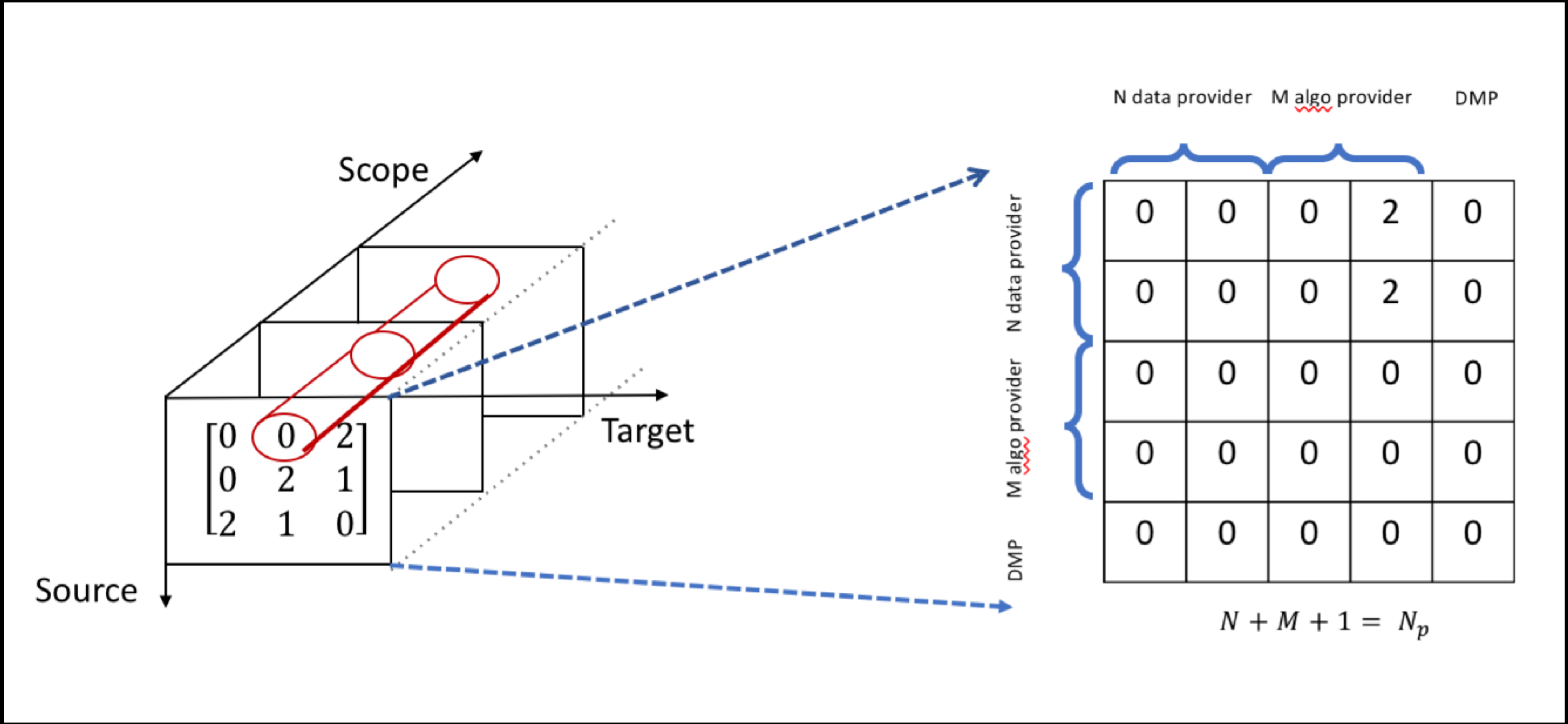
DMP archetypes and their representation



On the left one of the many collaboration models within a DMP. We call this archetype. One DMP can support multiple archetypes depending on the contracts between partners.

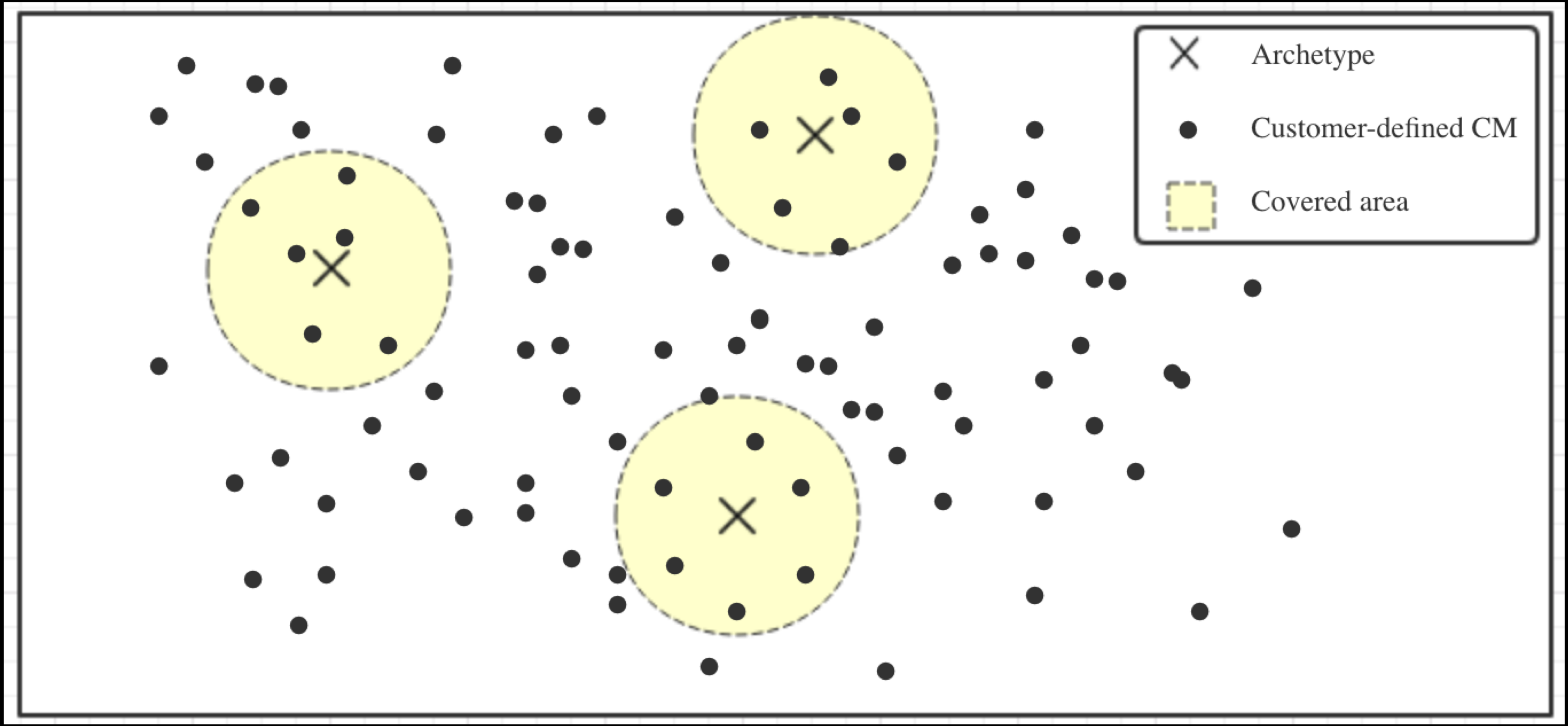
To match application/user requests to the archetype we need to model the archetype on the left in generic ways.

Models for archetypes



Parties in the DMP collaborate across a number of scopes: data, computing and output. They share data, they share algorithms and they can share results. The matrix on the left represent the level of collaboration between two parties in each of the scope. In the previous slide we had four parties plus the DMP exchange, so we have a 5x5 matrix.

Matching requests



Our work is to match a customer application to the ‘closest archetype’.

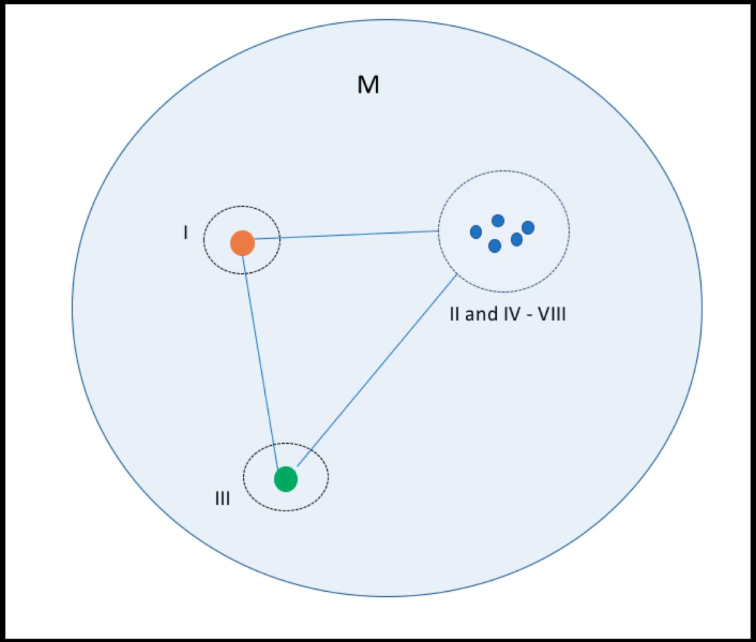
Dimensions of DMP

Coverage

How well can we satisfy users request with the available archetypes?

Extensibility

Can a DMP provide more archetypes to user?



Precision

How well the archetype database of a given DMP fits a request by customer?

Flexibility

How easily the requests from potential customers could be satisfied?

We defined four metrics to determine the 'richness' of a DMP.

Q&A

- More information:
  - http://delaat.net/dl4ld and http://delaat.net/epi
  - https://towardsamdex.org
- Contributions from:
  - Leon Gommans, Wouter Los, Paola Grosso, Yuri Demchenko, Lydia Meijer, Tom van Engers, Reggie Cushing, Ameneh Deljoo, Sara Shakeri, Lu Zhang, Joseph Hill, Lukasz Makowski, Ralph Koning, Gleb Polevoy, Tim van Zalingen, and many others!

dutch
digital
delta

Data Hub System Applicability

Industry

- Cross Cutting Field lab
- Innovation with SURF

smart industry
DUTCH INDUSTRY FIT FOR THE FUTURE

Science

- European Open Science Cloud
- FAIR model
    - Findable – Accessible – Interpretable - Reusable

EOSC pilot
The European Open Science Cloud for Research Pilot Project

Society

- Smart Cities & Arena
- Streaming Data Decision Support

Experimental Setup

Data Transfer nodes at UvA, KLM and Equinix
Running Kubernetes with a number of dockers (pods) see below.

```
tim@uva-kube-04:~$ kubectl get pods -o wide
NAME                              READY   STATUS    RESTARTS   AGE   IP              NODE           NOMINATED NODE
be2-deployment-c87646848-wt8l5    1/1     Running   0          77m   192.168.5.39    eqx-kube-03    <none>
mq1                               1/1     Running   0          13d   192.168.1.2     uva-kube-02    <none>
oex.airfrance                     1/1     Running   0          10d   192.168.4.16    eqx-kube-02    <none>
oex.klm                           1/1     Running   0          10d   192.168.3.5     eqx-kube-01    <none>
oex.trusted                       1/1     Running   0          13d   192.168.1.3     uva-kube-02    <none>
planner1                          1/1     Running   0          10d   192.168.4.15    eqx-kube-02    <none>
```

- be2 is the backend for the website.
  - It serves the static pages and passes new information and input to the planner.
- mq1 is the message queue that each oex writes logs to.
- oex.* each is one zone or 'object exchange server'.
  - It is responsible for handling requests from others and sending requests to other parties.
  - It should do so in accordance with a preselected contract/archetype.
- planner1 handles requests from be2 when selecting an archetype (and passes it on to the oex's) and when an application or pipeline is started (and passes it on to the oex).

DataHarbours: Computing archetypes for digital marketplaces

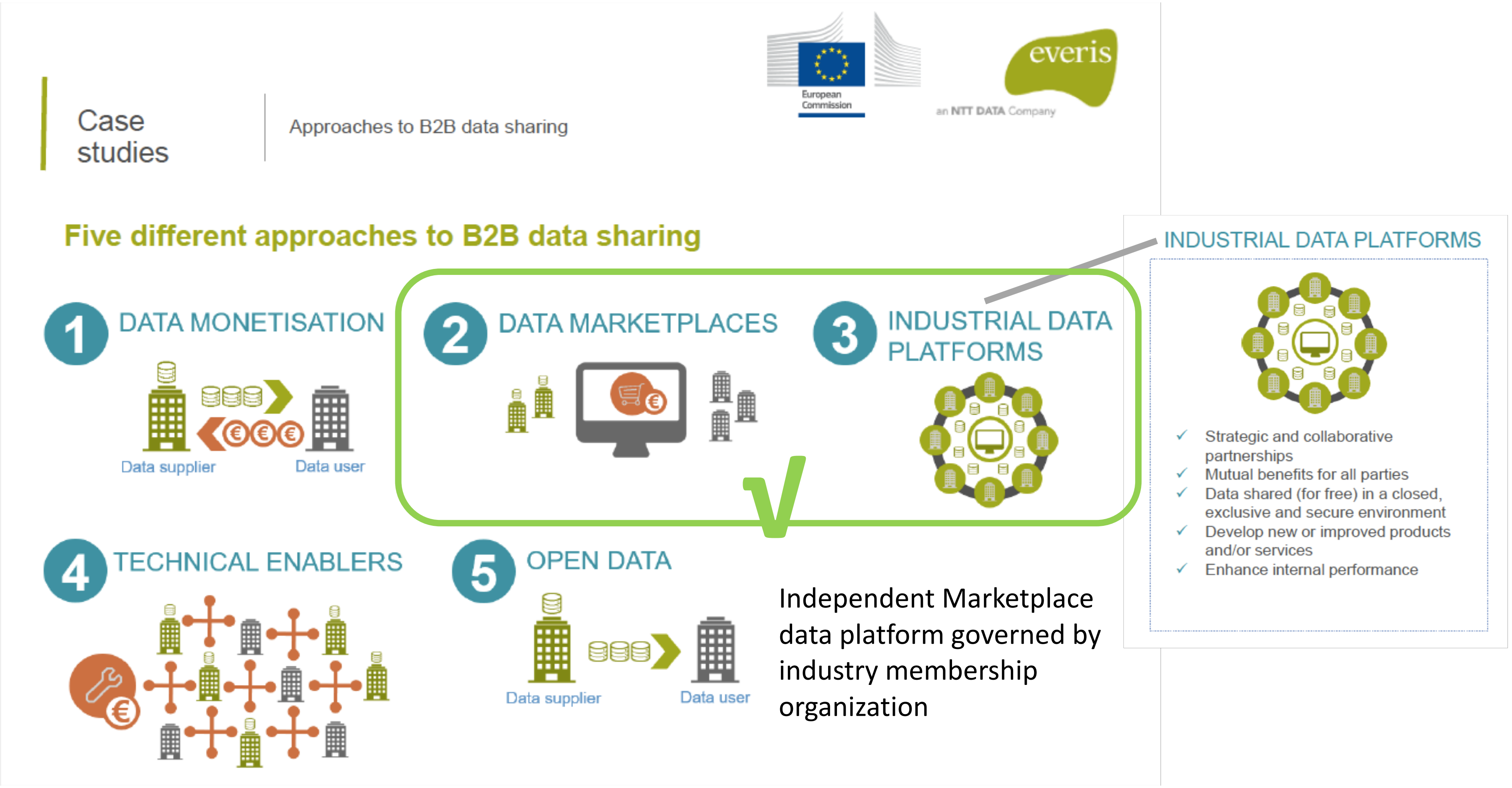
Reggie Cushing, Tim van Zalingen, Joseph Hill, Lu Zhang, Paola Grosso,
Cees de Laat, Leon Gommans, Vijaay Doraiswamy, Purvish Purohit,
Kaladhar Voruganti, Craig Waldrop, Rodney Wilson, Marc Lyonnais

SAE Use Case envisaged **research** collaboration

Funding Agency	NSF — Big Data Hub / Spoke or Industry initiative funding			NWO Netherlands Organisation for Scientific Research — Topsector Funding
International Networking	Internet2, ESnet Energy Sciences Network			GÉANT
Regional / National Networking	CENIC Connecting California	SoX Southern Crossroads	LEARN Lonestar Education and Research Network	SURFNET
Local University	Stanford	Georgia Tech	UT Dallas	Universiteit van Amsterdam
Aircraft MRO, OEM & Operators	Boeing	Delta Air Lines	Bell Helicopter	Air France KLM
Industry Standards Body	SAE International — SAE AeroSpace Group HM-1 working group Use Case on aircraft sensor Big Data			

data Sharing approach: Combine 2&3

MANAGED BY AN INDEPENDENT INDUSTRY MEMBERSHIP ORGANIZATION



Independent Marketplace data platform governed by industry membership organization

https://publications.europa.eu/en/publication-detail/-/publication/8b8776ff-4834-11e8-be1d-01aa75ed71a1/language-en