# Provenance-based System Accountability

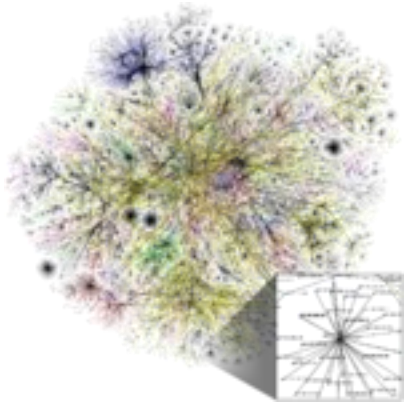
Luc Moreau
Web and Internet Science
Electronics and Computer Science
University of Southampton

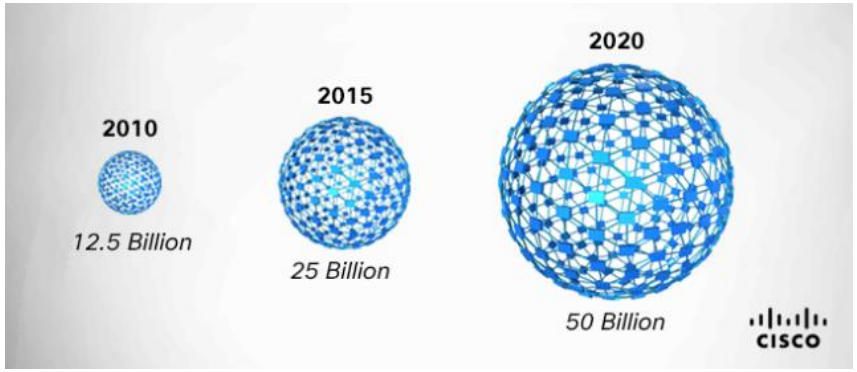
Trung Dong Huynh, Amir Sezavar Keshavarz, Danius Michaelides, Heather Packer, Darren Richardson, Jamal Hussein, Mimie Liotsiou, Faranak Hardcastle, Mufy Ali

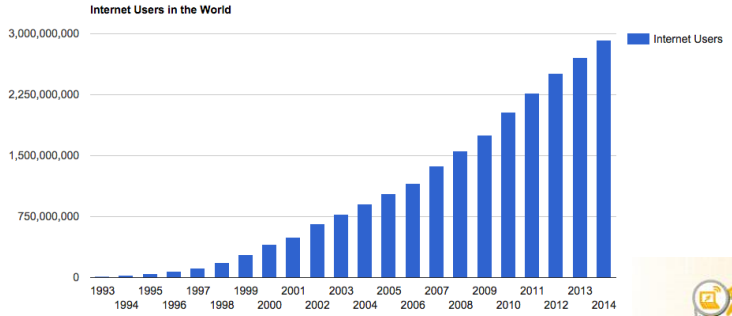
# Overview

- Context: The case for provenance
- Provenance Introduction
- PROV: a W3C Standard for Provenance
- A Crowdsourcing Illustration
- Applications of Provenance
- Future directions and Conclusions

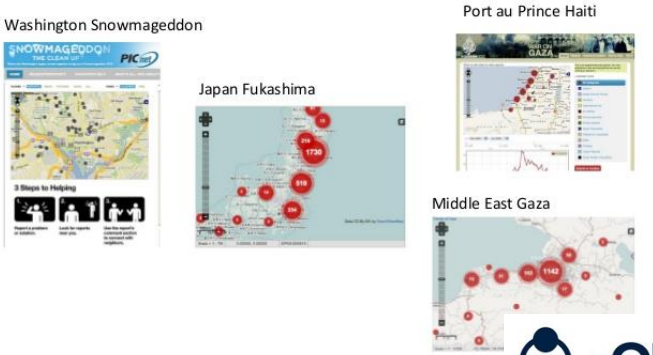
# The Era of Connectivity: People, Devices






Variants of the
Ushahidi Social Machine




SOCIAM
Social Machines

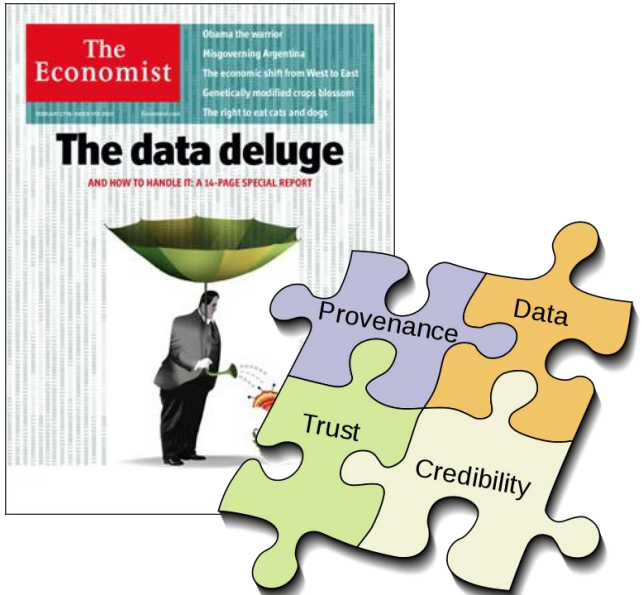
Smart Society
Hybrid Collective Adaptive Systems

ORCHID
Human Agent Collectives

# Mother's Home Cooking vs Street Food

JP Rangaswami, CDO @ Deutsche Bank

- Devices provide information:
  - from an ever more diverse range of  sources, via ever more sensor types
  - that measures ever more of everything
  - that can be mashed-up in unforeseen ways




How to make informed decision?

# (Information, System, People) Accountability

- Accountable:
  - "required or expected to justify actions or decisions"
- Participants AND social machines to be held accountable
  - transparent and accountable social machines
    - increase a participant's understanding of the machine's processes, and
    - can increase the participant's trust of the social machine
  - a description of what participants do
    - enables participants to feel that their actions can be monitored
    - incentive to conduct themselves in a respectable manner.

'Bogus' AP tweet about explosion at the White House wipes billions off US markets

The FBI and SEC are to launch investigations after more than £90bn was temporarily wiped off the US stock market when hackers broke into the Twitter account of the Associated Press and announced that two bombs had exploded at the White House, injuring Barack Obama.

351 154 0 5 510 Email

Weitzner et al

# Algorithms Accountability and Transparency

## USACM 7 principles

**1. Awareness:** Owners, designers, builders, users, and other stakeholders of analytic systems should be aware of the possible biases involved in their design, implementation, and use and the potential harm that biases can cause to individuals and society.

**2. Access and redress:** Regulators should encourage the adoption of mechanisms that enable questioning and redress for individuals and groups that are adversely affected by algorithmically informed decisions.

**3. Accountability:** Institutions should be held responsible for decisions made by the algorithms that they use, even if it is not feasible to explain in detail how the algorithms produce their results.

**4. Explanation:** Systems and institutions that use algorithmic decision-making are encouraged to produce explanations regarding both the procedures followed by the algorithm and the specific decisions that are made. This is particularly important in public policy contexts.

**5. Data Provenance:** A description of the way in which the training data was collected should be maintained by the builders of the algorithms, accompanied by an exploration of the potential biases induced by the human or algorithmic data-gathering process. Public scrutiny of the data provides maximum opportunity for corrections. However, concerns over privacy, protecting trade secrets, or revelation of analytics that might allow malicious actors to game the system can justify restricting access to qualified and authorized individuals.

**6. Auditability:** Models, algorithms, data, and decisions should be recorded so that they can be audited in cases where harm is suspected.

**7. Validation and Testing:** Institutions should use rigorous methods to validate their models and document those methods and results. In particular, they should routinely perform tests to assess and determine whether the model generates discriminatory harm. Institutions are encouraged to make the results of such tests public.

# PROVENANCE

# Provenance for food, art, and beyond


"Good curation demands good provenance. Provenance is no longer merely the nicety of artists, academics, and wine makers. It is an ethic we expect." (Jeff Jarvis)

http://buzzmachine.com/2010/06/27/the-importance-of-provenance/

# Beyond Provenance for food and art

## Open Data and Journalism

- Data wrangling can introduce errors, data journalists should care about the validity of data; provenance of data should include its primary source, but also all the transformational steps performed by anyone.

http://datadrivenjournalism.net/featured_projects/how_spending_stories_spots_errors_in_public_spending

## Accountability, Transparency, Compliance

- Steve New refers to the provenance of a company's products, and explains how businesses have changed their practice to make their supply chain transparent, because they worry about quality, safety, ethics, and environmental impact.

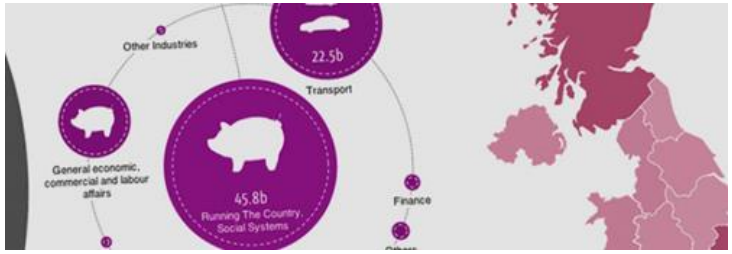
http://hbr.org/2010/10/the-transparent-supply-chain/ar/1

## Reproducibility of Science

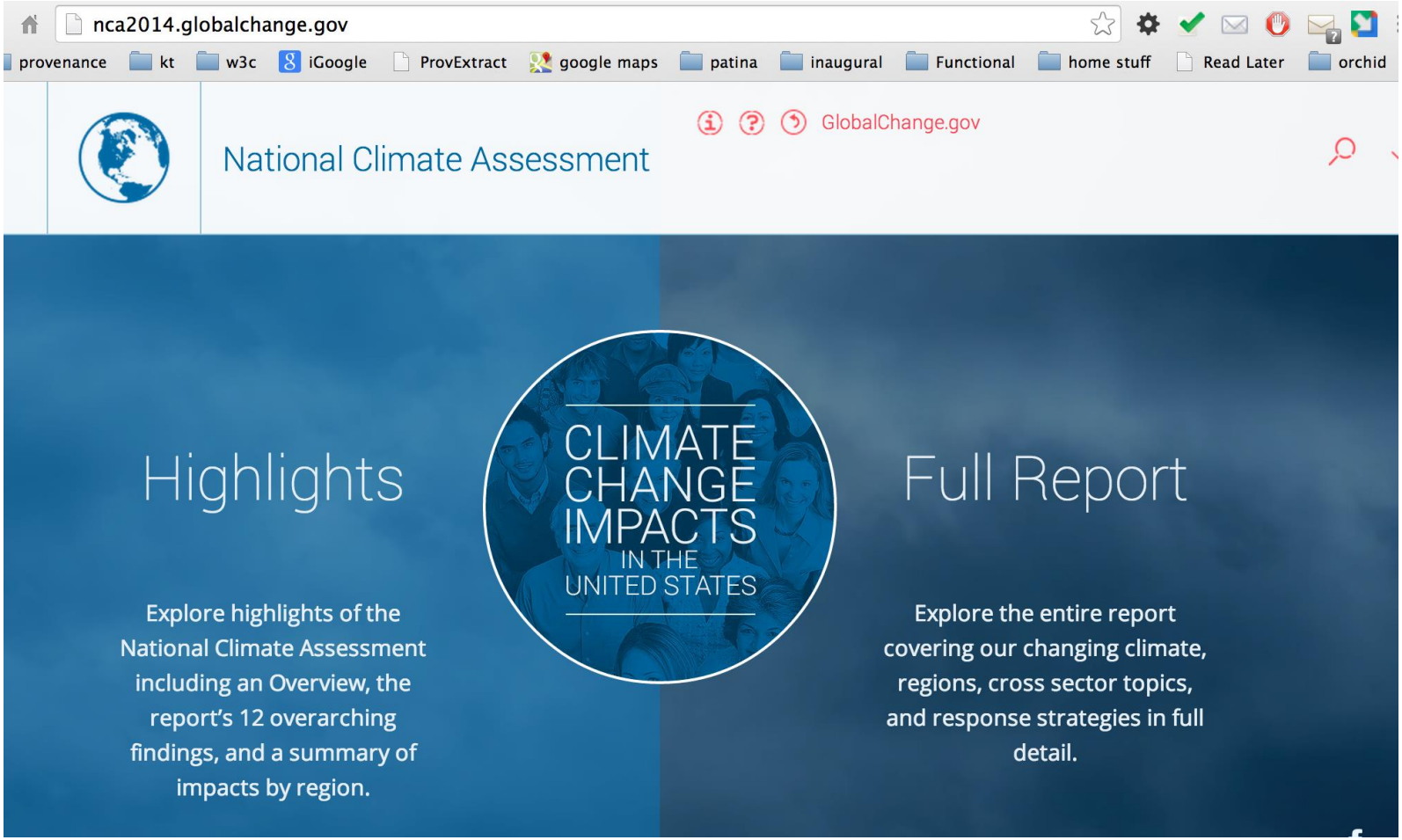
- Provenance is the equivalent of a logbook

capturing all the steps involved in the derivation of a result,

could be used to replay the execution that led to that result so as to validate it.



# National Climate Assessment



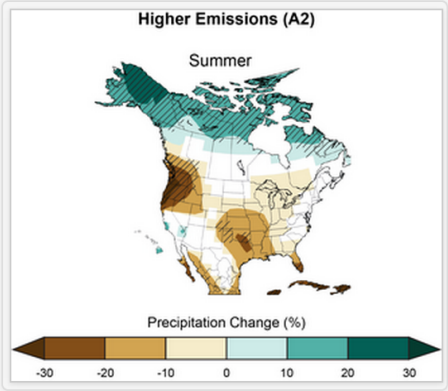
http://nca2014.globalchange.gov/report/our-changing-climate/precipitation-change#graphic-16689

data.globalchange.gov/image/1a061197-95cf-47bd-9db4-f661c711a174

provenance | kt | w3c | iGoogle | ProvExtract | google maps | patina | inaugural | Functional | home stuff | Read Later

# image : 1a061197-95cf-47bd-9db4-f661c711a174

## Projected Precipitation Change by Season (Summer)




*Cooperative Institute for Climate and Satellites - NC*
Kenneth Kunkel

The time range for this image is January 01, 1971 (00:00 AM) to December 31, 2099 (23:59 PM).

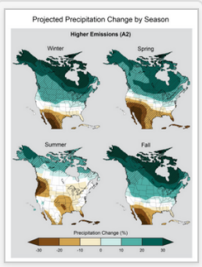
This image was created on July 24, 2013.

The spatial range for this image is 18.14° to 82.31° latitude, and -165.94° to -53.44° longitude.

Attributes : Precipitation, projections, seasonal, CMIP3, A2.

This image was derived from dataset nca3-cmip3-r201205 using the activity 1a061197-nca3-cmip3-r201205-process.

This image is part of this figure :



2.14

<http://data.globalchange.gov/image/1a061197-95cf-47bd-9db4-f661c711a174>
<http://www.w3.org/ns/prov#wasDerivedFrom>
<http://data.globalchange.gov/dataset/nca3-cmip3-r201205> .

# The Gazette

https://www.thegazette.co.uk/notice/2152652

Home | All notices | Wills and Probate | Insolvency | Publications | Data | Validation | Shop | Register | Sign in

THE GAZETTE
OFFICIAL PUBLIC RECORD

Published by Authority | Est 1665

All notices | News | Resources

## Notice details

**Type:**
Partnerships
> Change in the Members of a Partnership

**Publication date:**
25 June 2014, 19:23

**Edition:**
The London Gazette

**Notice ID:**
2152652

**Notice code:**
2701

## Change in the Members of a Partnership

### Inghams Solicitors

Notice is hereby given that Bradley Robert Burrow retired as a Partner from the Partnership known as Inghams Solicitors, 4-8 Leopold Grove, Blackpool, Lancashire FY1 4JR (Head Office), on 30 June 2014. The remaining partners comprising Peter John Isaacs, John Philip Muir, Richard John Harvey Stratham, Diane Marie Killey, Christopher Barry Beckett and Andrew Paul Weaver will continue to carry on the business of Inghams Solicitors from the Partnership Offices in Blackpool, Bispham, Clevelys, Poulton-Le-Fylde and Fleetwood.

Signed on behalf of the Partners of Inghams Solicitors

*Bradley R Burrow*, Partner

19 June 2014

BACK

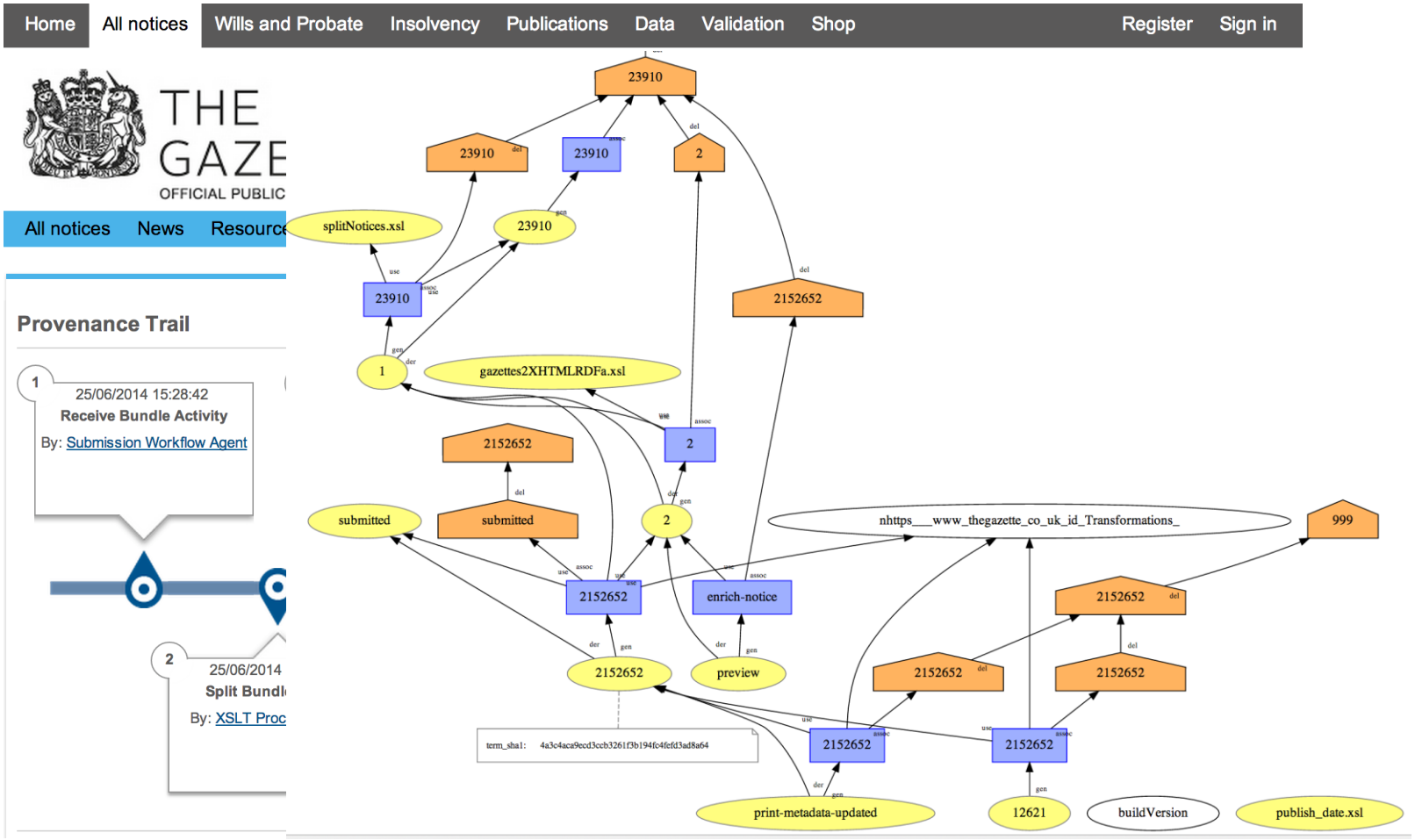
## Actions

- Save notice to My Gazette
- Print notice
- Share this notice
- Linked data view
- Provenance trail

## Digital Signature

- Signed Document HTML
- Signature for HTML Document
- Signed RDF Document
- Signed Provenance RDF
- What is a digital signature?

# Gazette Provenance



# Provenance Definition

- Oxford English Dictionary:
  - the fact of coming from some particular source or quarter; origin, derivation
  - the history or pedigree of a work of art, manuscript, rare book, etc.;
  - concretely, a record of the passage of an item through its various owners.

- World Wide Web Consortium:

Provenance is a record that describes the people, institutions, entities, and activities, involved in producing, influencing, or delivering a piece of data or a thing in the world

# PROV

# Provenance Working Group

W3C Technology and Society domain

W3C PROV

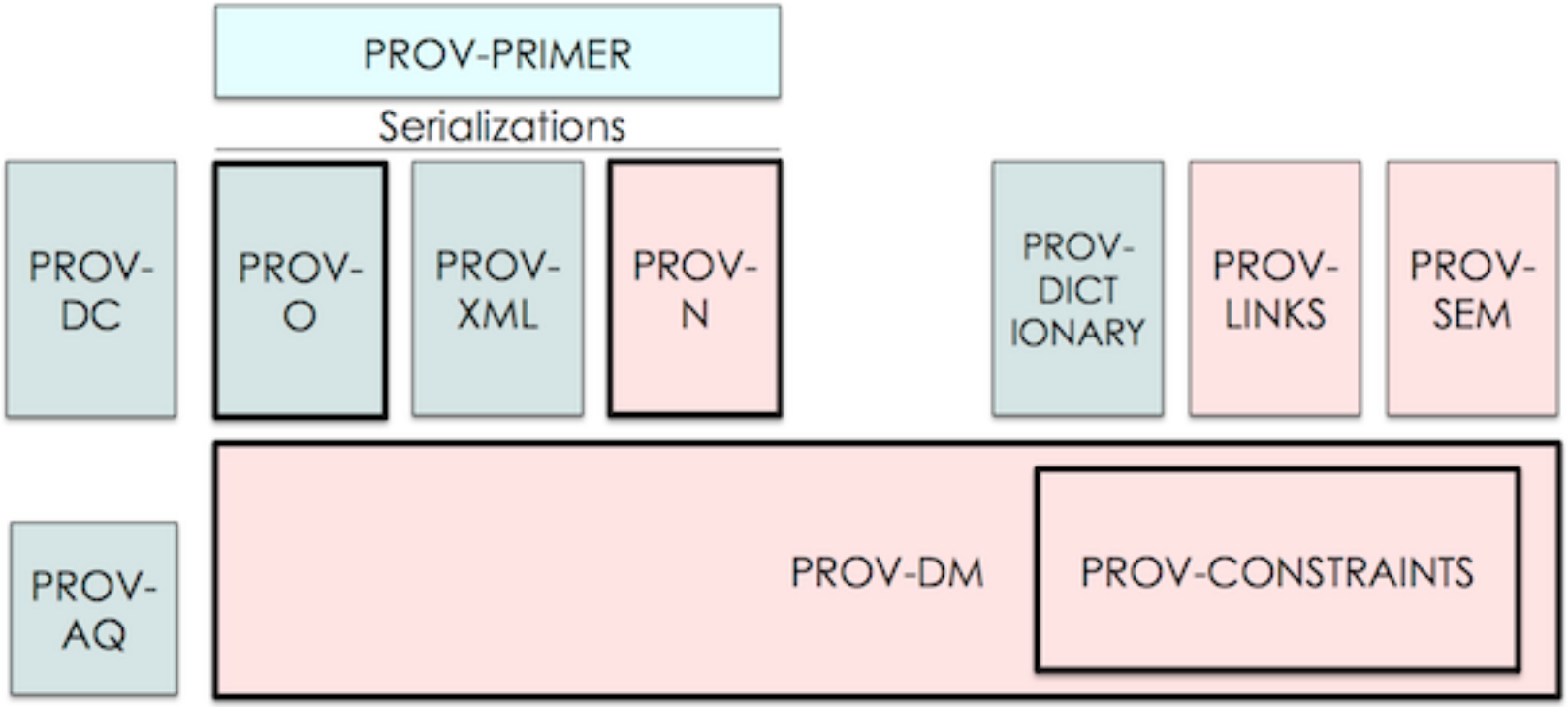
## Provenance Interchange Working Group Charter

The **mission** of the Provenance Working Group, part of the Semantic Web Activity, is to support the widespread publication and use of provenance information of Web documents, data, and resources. The Working Group will publish W3C Recommendations that define a language for *exchanging* provenance information among applications.

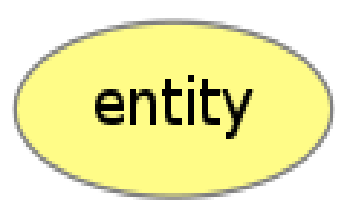
Join the Provenance Working Group.

| | |
|---|---|
| **End date** | 1 October 2012 |
| **Confidentiality** | Proceedings are public |
| **Initial Chairs** | Luc Moreau, University of Southampton<br>Paul Groth, VU University Amsterdam |
| **Initial Team Contacts (FTE %: 20)** | Sandro Hawke |
| **Usual Meeting Schedule** | Teleconferences: Weekly<br>Face-to-face: Once Annually |

# PROV: abstract model and serializations

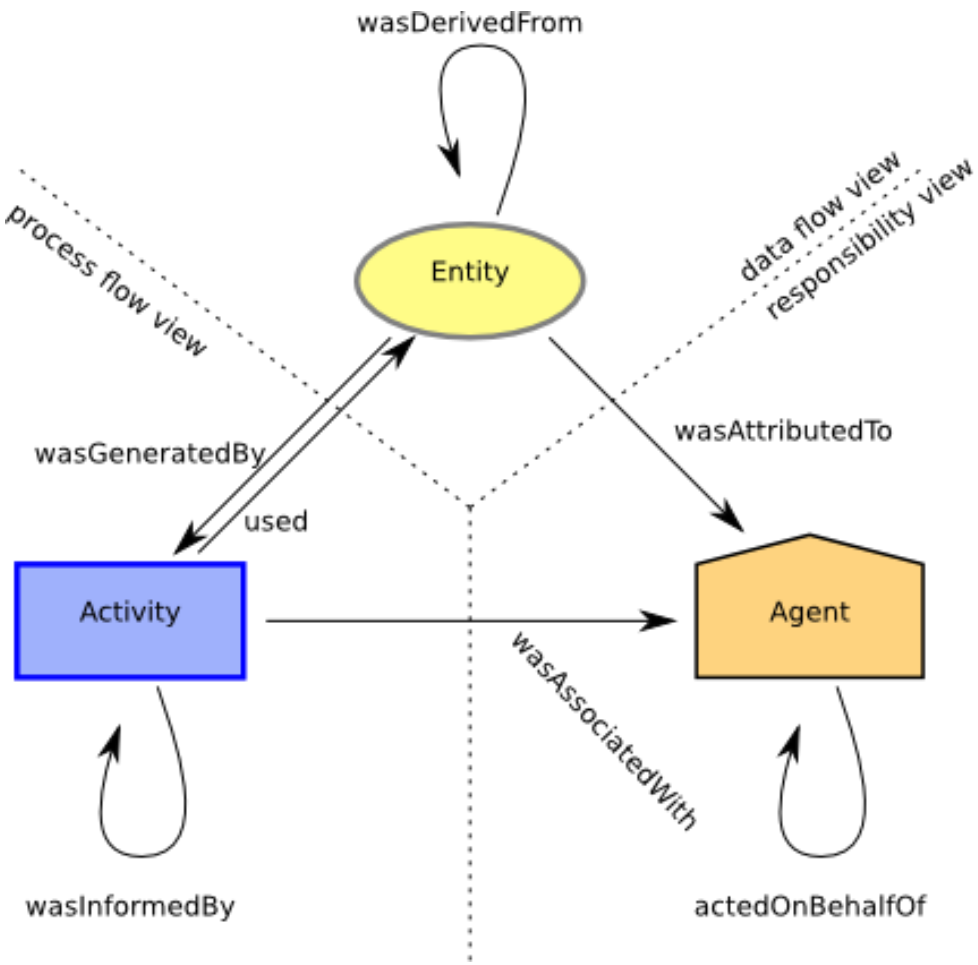


# Three Core Concepts

| Social Machine | PROV |
|---|---|
| Piece of information, decision, vote, document |   |
| Actions such as voting, writing, reporting, commenting, approving |   |
| Person, service, system, organization, collective |   |

http://www.w3.org/TR/prov-dm/

# Three Views of Provenance



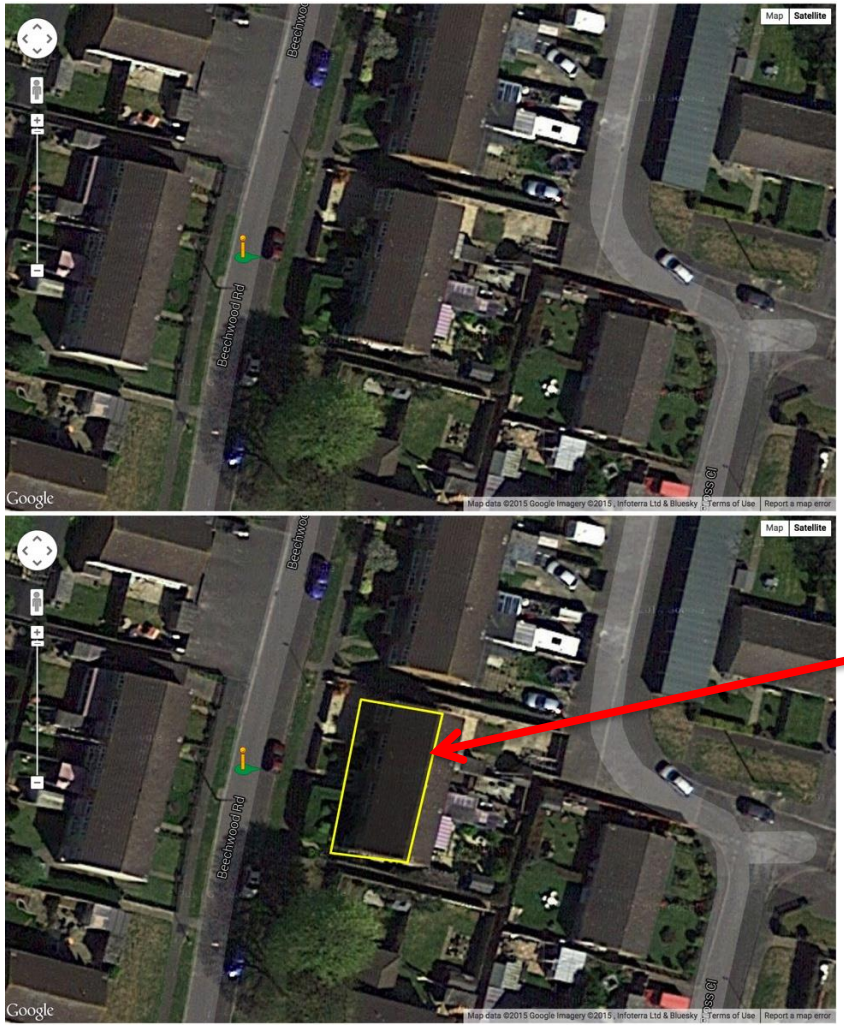
**Highlight**.

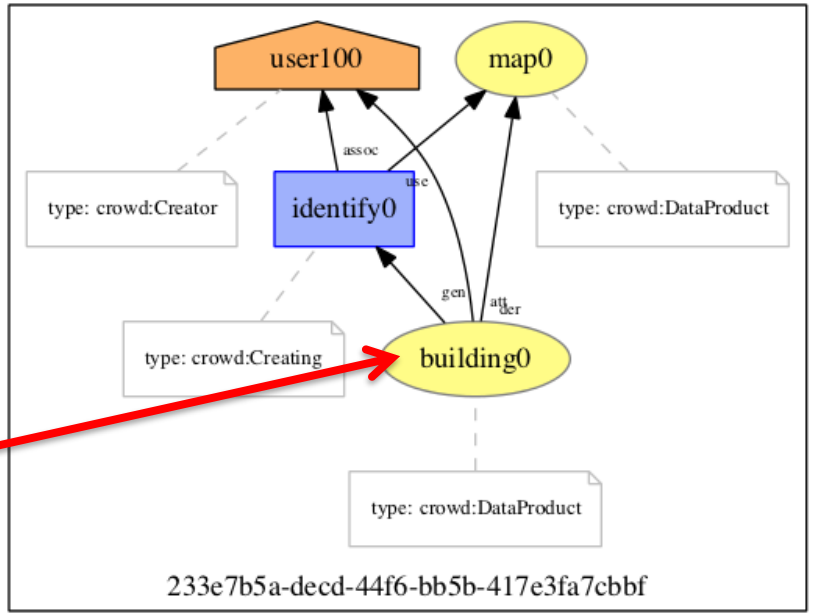
This application involves users from the “crowd”.

Provenance allows their interactions with the system to be audited and analysed.

# PROV IN PRACTICE: ILLUSTRATION

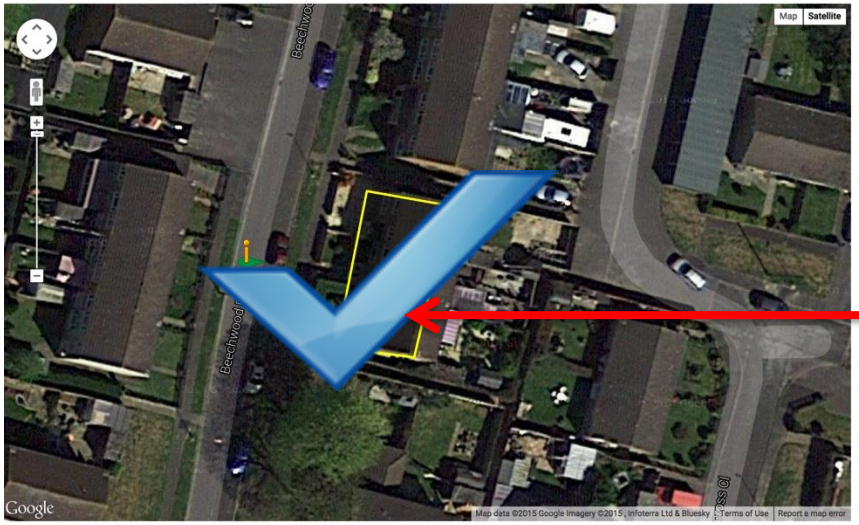
# Illustration: Building Identification

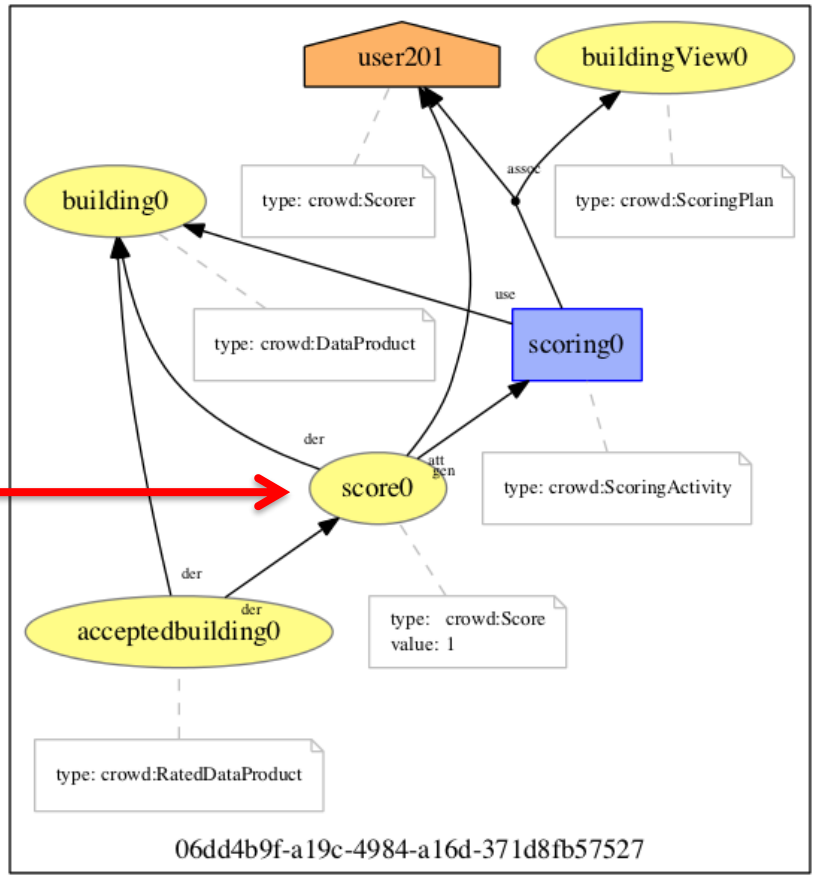


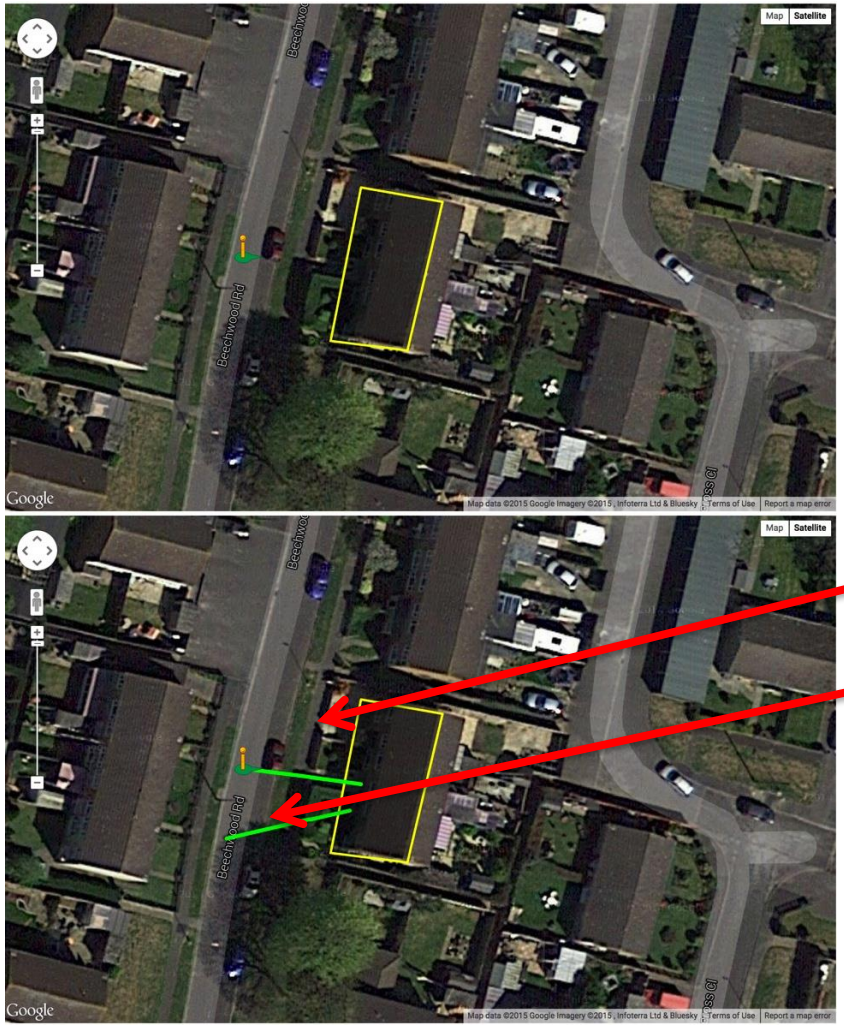

Ramchurn, S. D., Huynh, D. T., Venanzi, M., & Shi, B. (2013). Collabmap: crowdsourcing maps for emergency planning. In ACM Web Science.

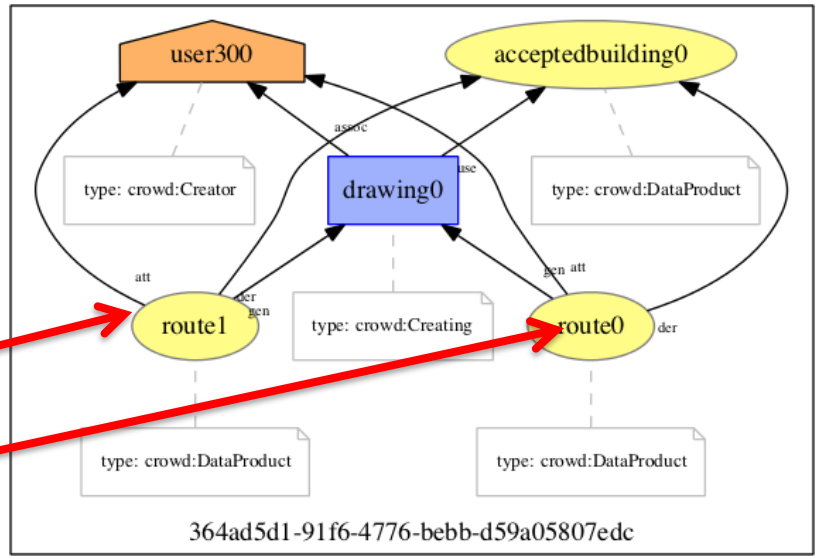
# Illustration: Building Scoring



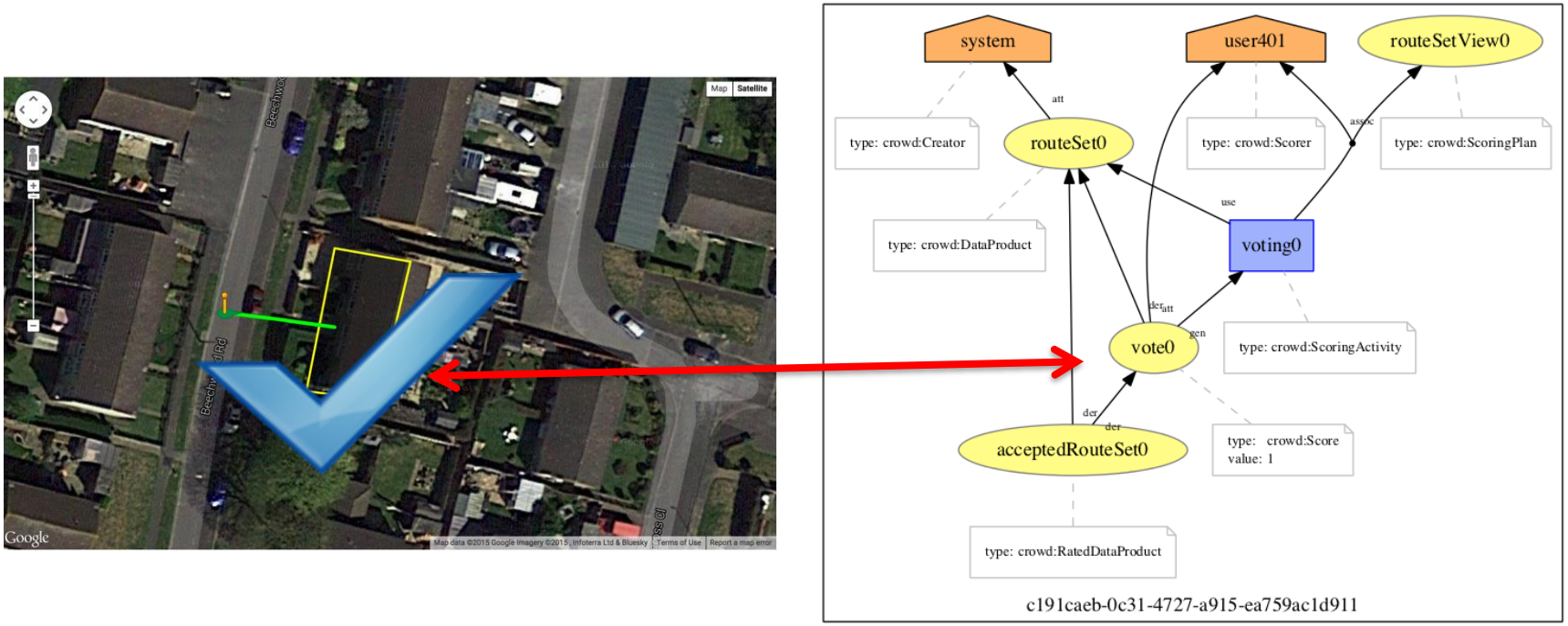



# Illustration: Route Drawing

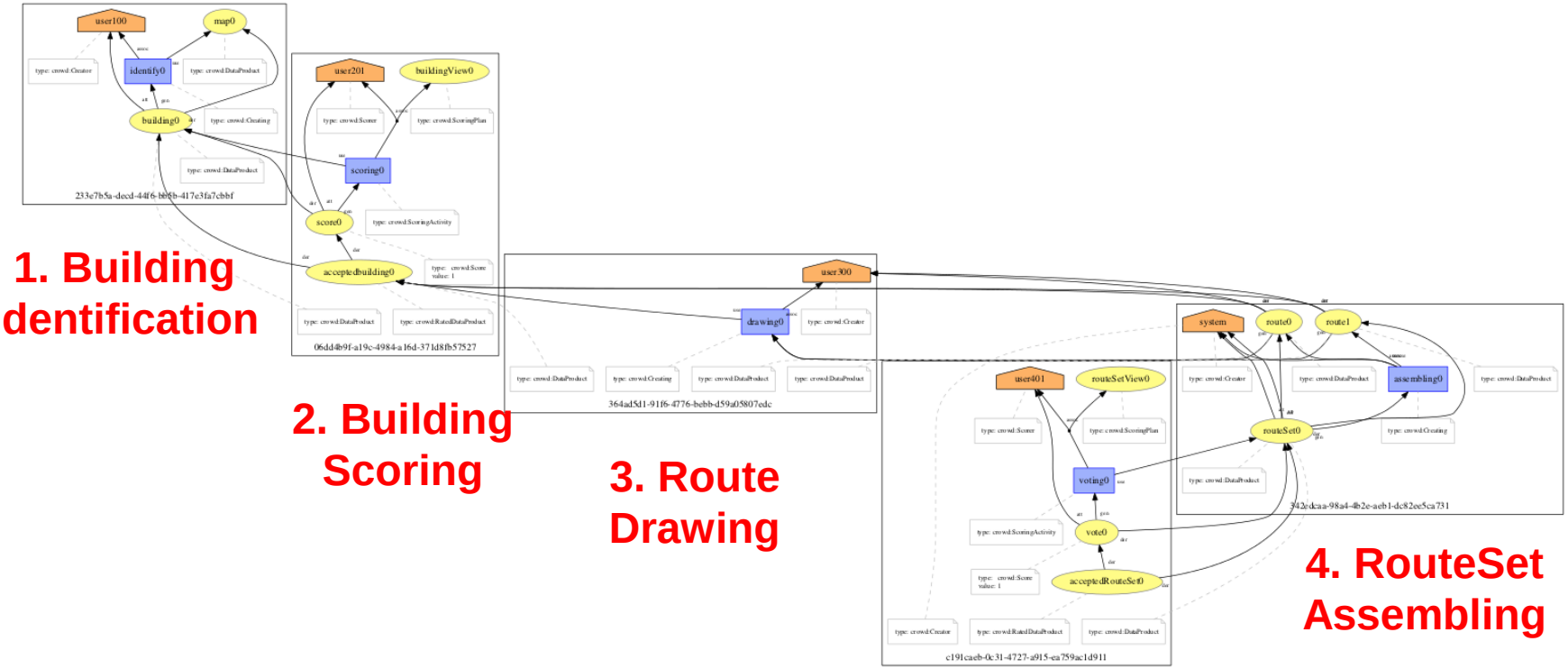


# Illustration: RouteSet Scoring



# Entire Workflow




1. Building Identification

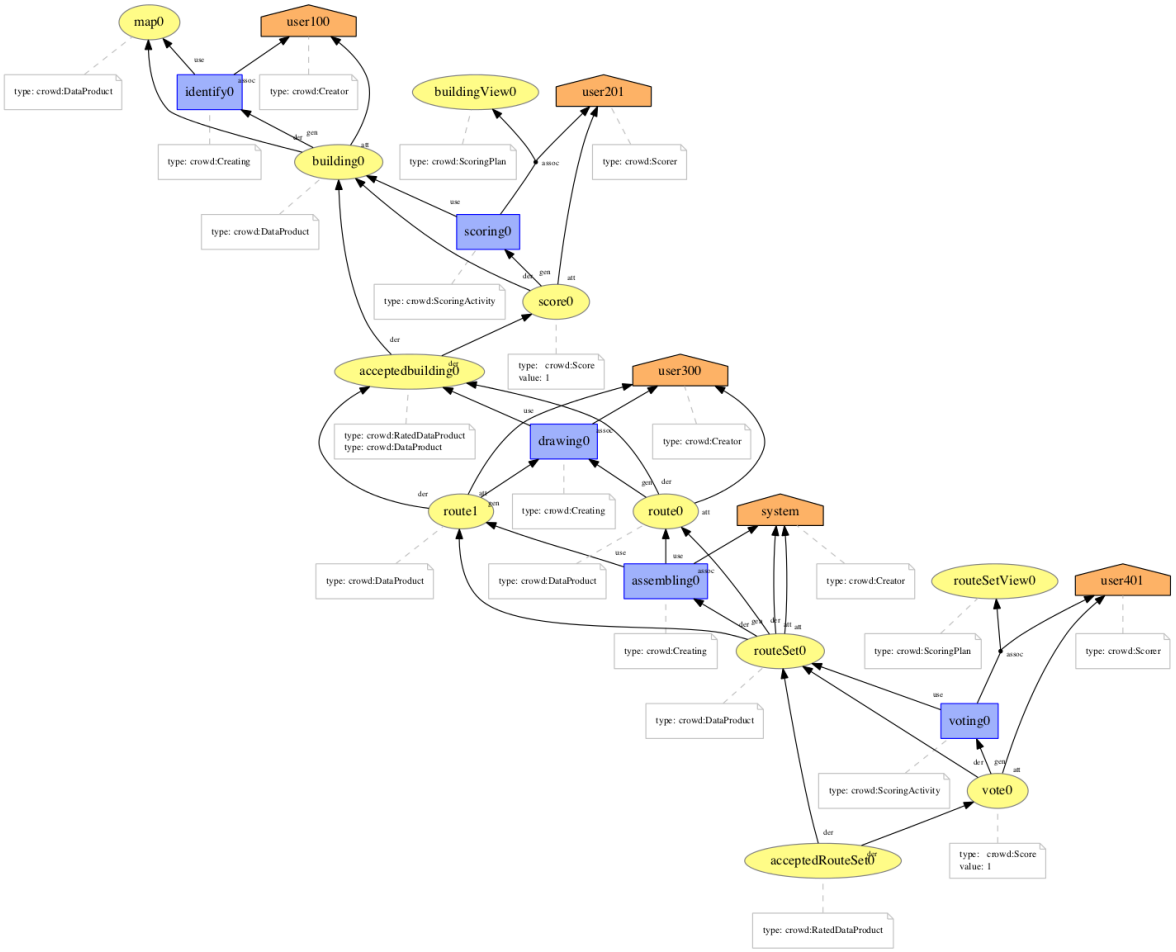
2. Building Scoring

3. Route Drawing

4. RouteSet Assembling

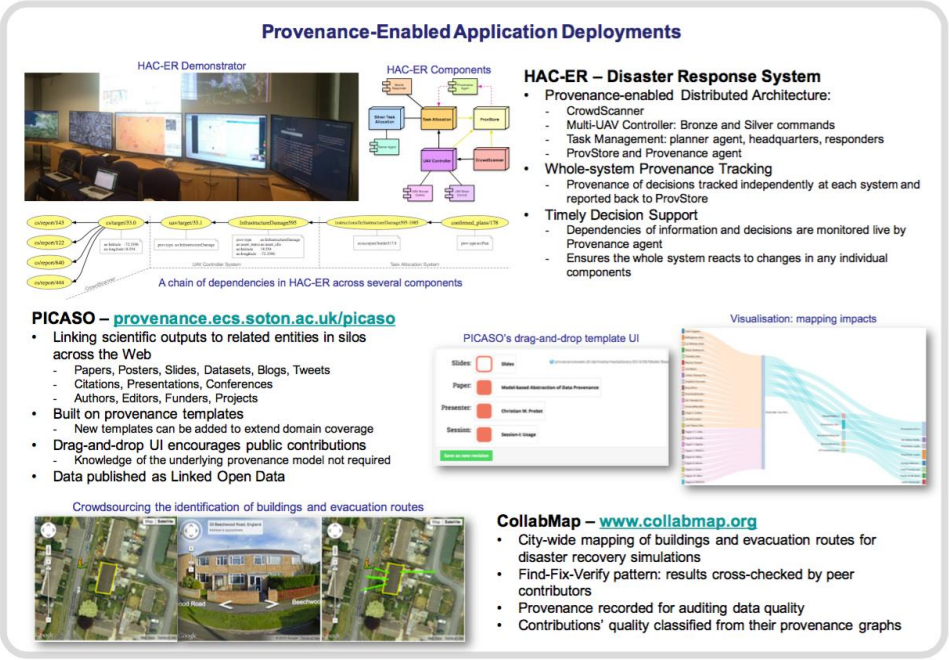
5. RouteSet Voting

# Entire Workflow (2)



# The Story so far

- PROV: standardised vocabulary to describe
  - Flow of data
  - Processes
  - Responsibility
- PROV allows systems to be enriched with “data lineage” showing the origin of data
- A huge step towards systems accountability
- … but what can we do beyond this with provenance?




Rideshare
Atomic Orchid
Collabmap
Food Provenance
Interactive Books
PICASO

# APPLICATIONS

**Highlight.**

Processes become very complex very quickly.

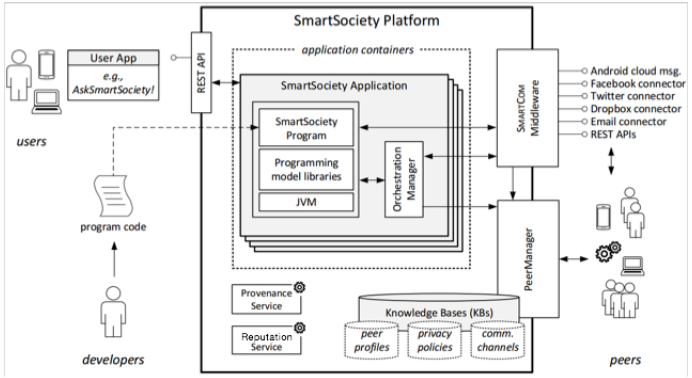
Ability to summarise, find common patterns, detect outliers

# RIDESHARE

In collaboration with Heather Packer

# Ride Sharing

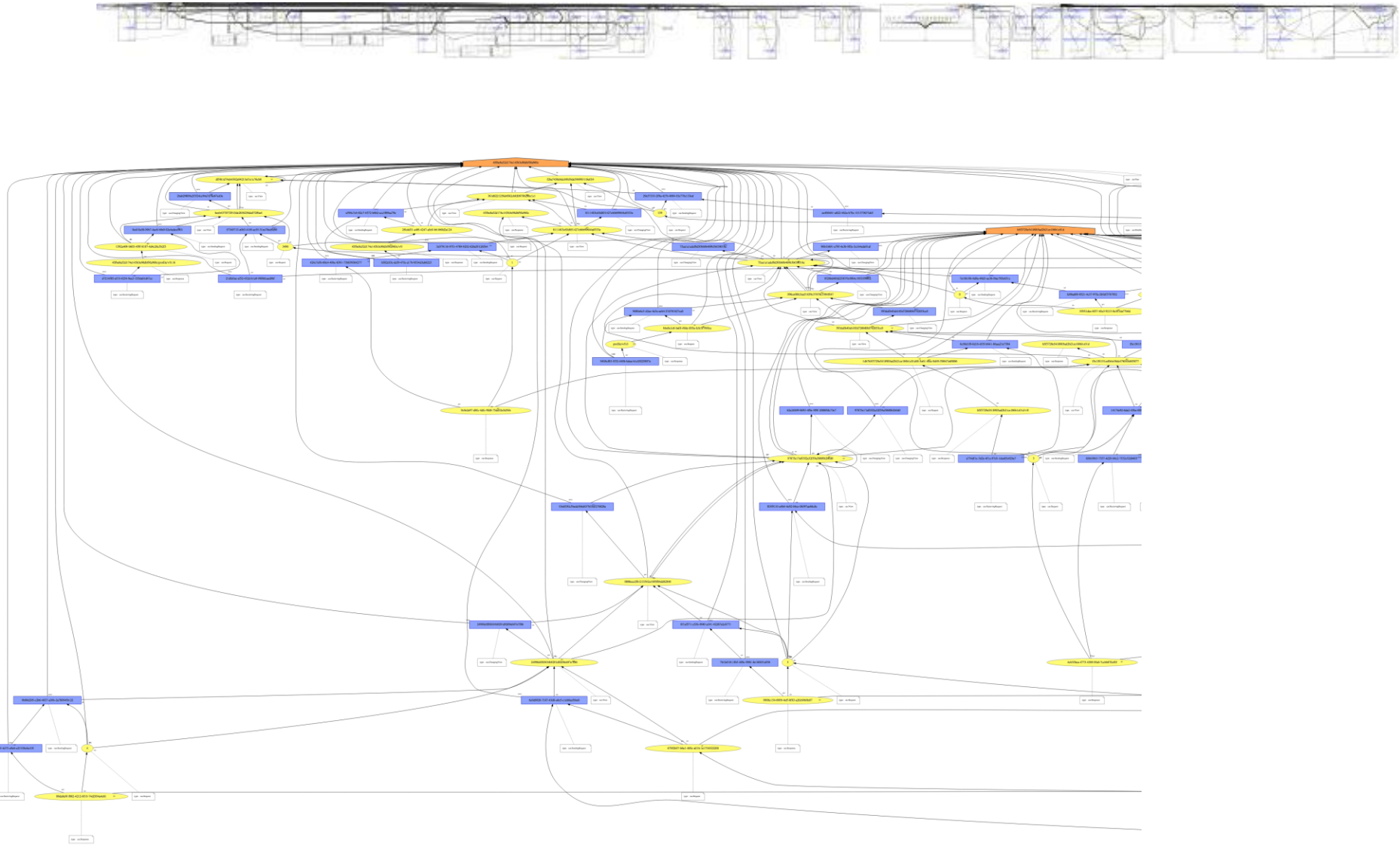
- Timely
- Challenging (security, coordination, availability)
- As a social machine: governance, privacy, accountability




## Why rideSharing?

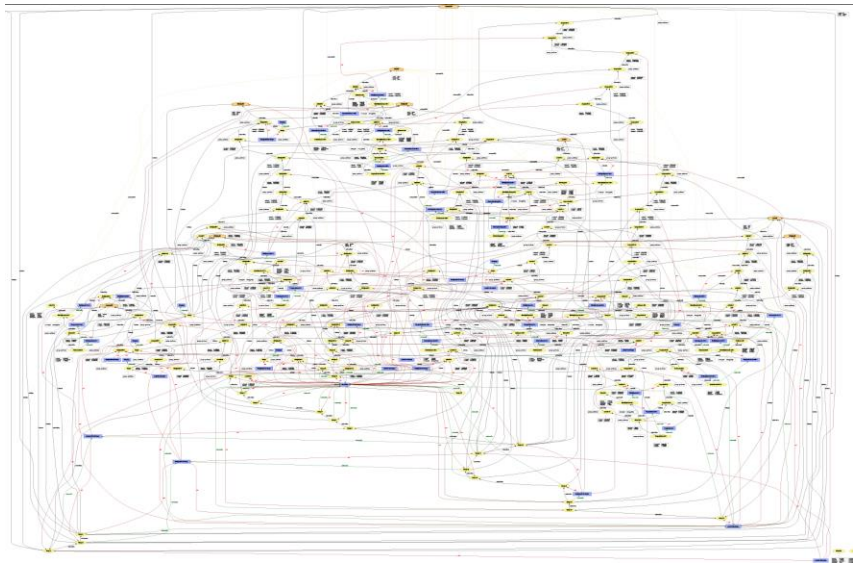
- Timely application
- Challenging problem
  - Security
  - Coordination
  - Availability
- Optimization must be
  - Human-oriented
  - Eco-friendly
  - Cost-effective


www.smart-society-project.eu

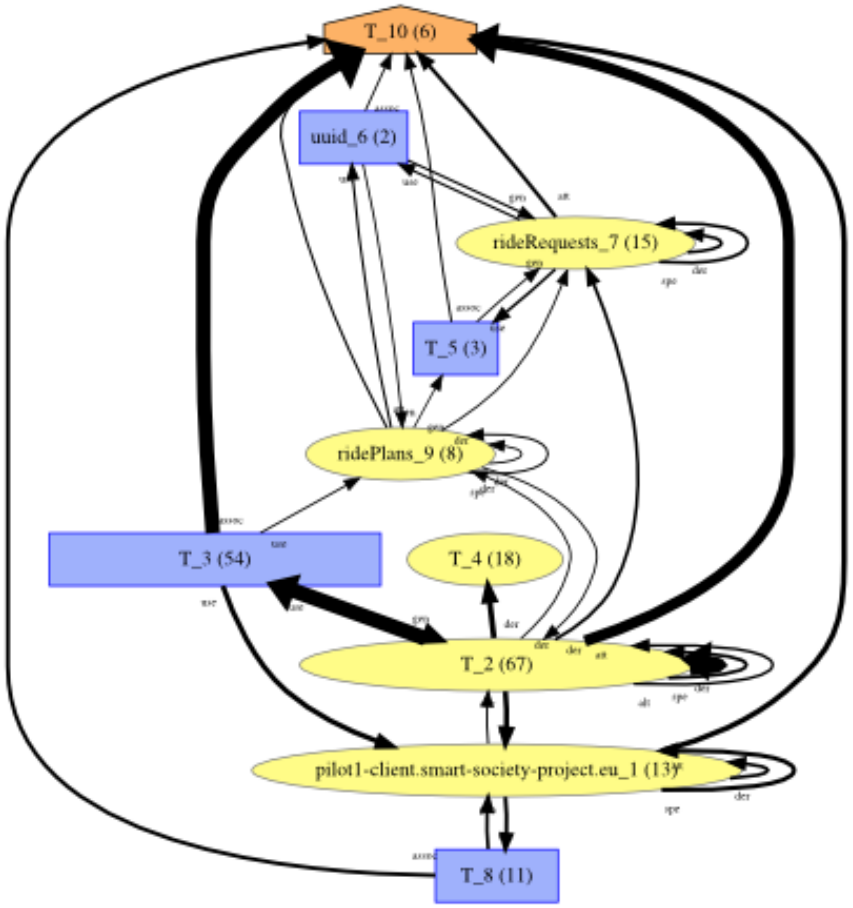


# Understanding Provenance at Scale

- Finding a needle in a haystack of provenance
- Requirements:
  - **Essence** of Provenance: a provenance summary should capture the essence of the provenance graph that it summarises.
  - **Outliers**: It should be possible to detect anomalies or outliers in a provenance summary
  - **Conformance**: It should be possible to decide whether a provenance graph is compatible, or conformant, with a provenance summary.



# Summarisation




- Clear Narrative
- Common Patterns
- Outliers

| | Original | Summary |
|---|---|---|
| Nodes | 188 | 10 |
| Edges | 456 | 36 |

- User submits (T_5) ride requests (T_7)
- They lead to negotiation (T_6) that creates ride plans (T_9)
- Response objects (T_2) are produced by UI Requests (T_3)
- Response objects (T_2) result in views (T_1) on the UIs

**Highlight.**

Knowledge about a situation evolves over time, and may be invalidated by new information.

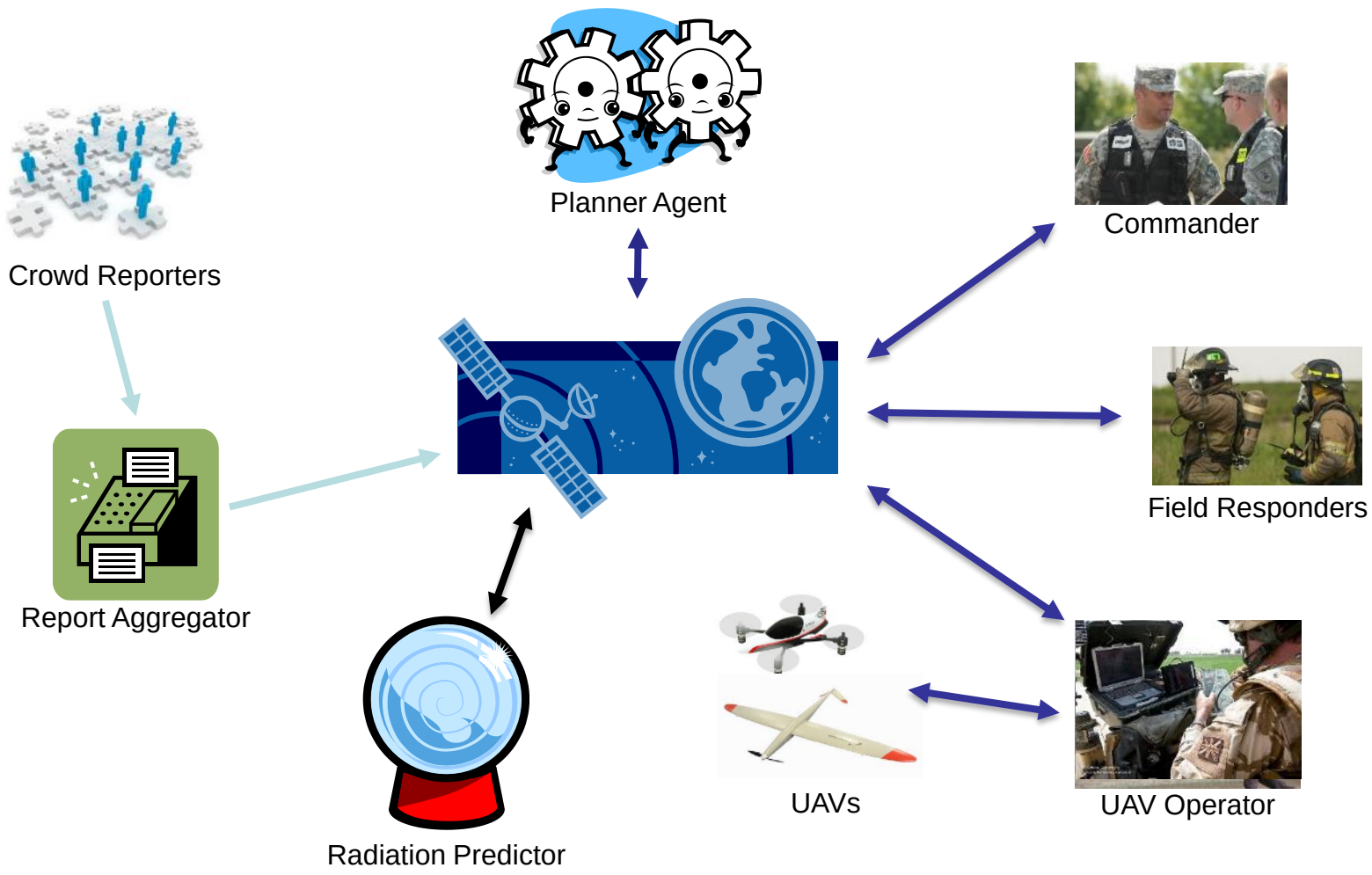
Notification of events and identification of dependencies.

# ORCHID EMERGENCY RESPONSE

In collaboration with Trung Dong Huynh

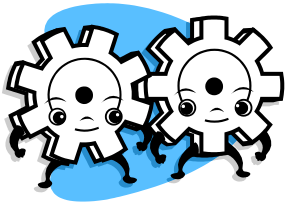
ORCHID

# Emergency Response



# Tracking Data

Report Aggregator



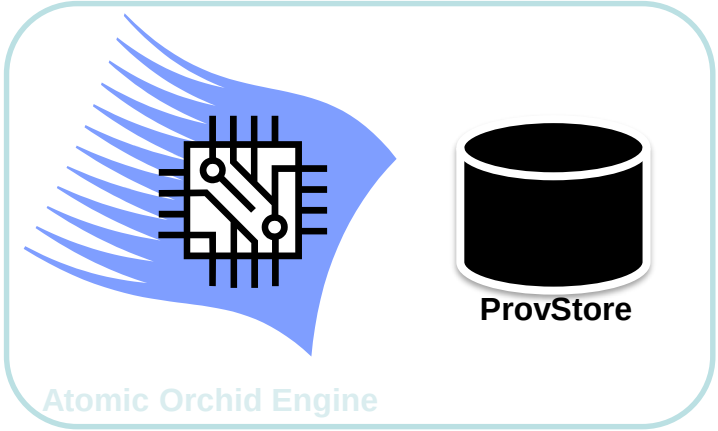
Planner Agent

UAVs

Radiation Predictor

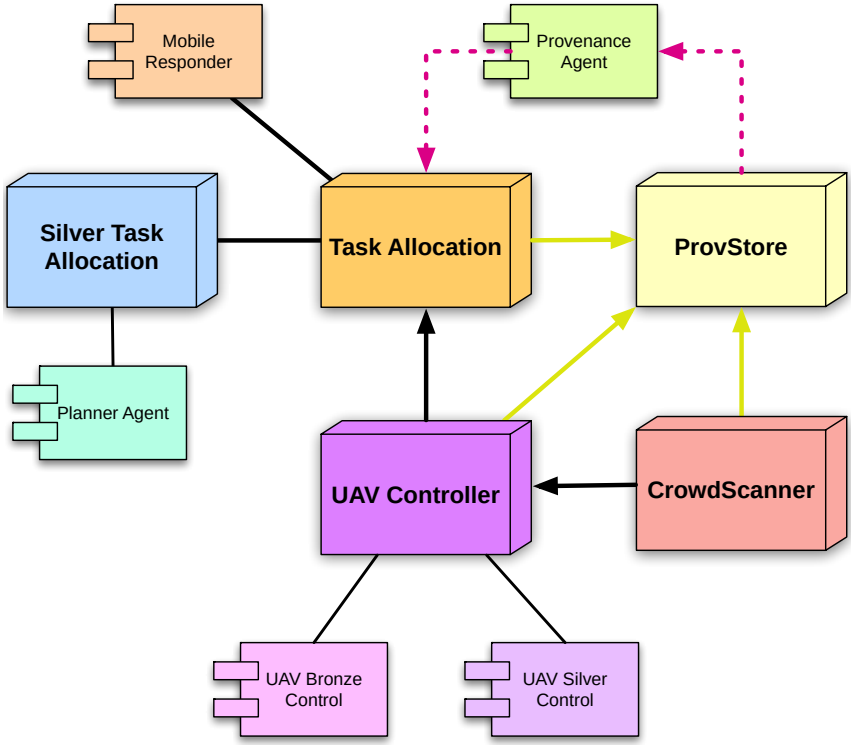

Mobile App

HQ Control



# Provenance-based Notifications

- Publish notifications about “events of interest” occurring in provenance graph, as they are being streamed
- Identify parts of the system that are affected




Ramchurn, Sarvapali, Simpson, Edwin, Fischer, Joel, Huynh, Trung Dong, Ikuno, Yuki, Reece, Steven, Jiang, Wenchao, Wu, Feng, Flann, Jack, Roberts, S.J., Moreau, Luc, Rodden, T. and Jennings, N.R. (2015) HAC-ER: A disaster response system based on human-agent collectives. In, *14th International Conference on Autonomous Agents and Multi-Agent Systems, Istanbul, TR, 04 - 08 May 2015.* , 533-541.

**Highlight**.
Behaviour can be regarded as suspicious, processes may be non performant, report can be unreliable.

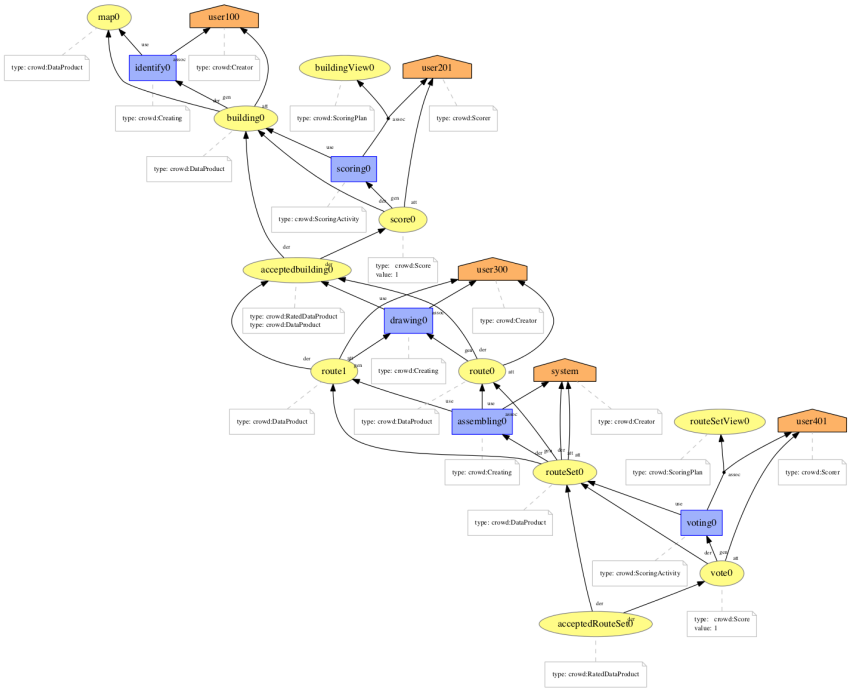
Build predictive models to label behaviour, processes or reports.

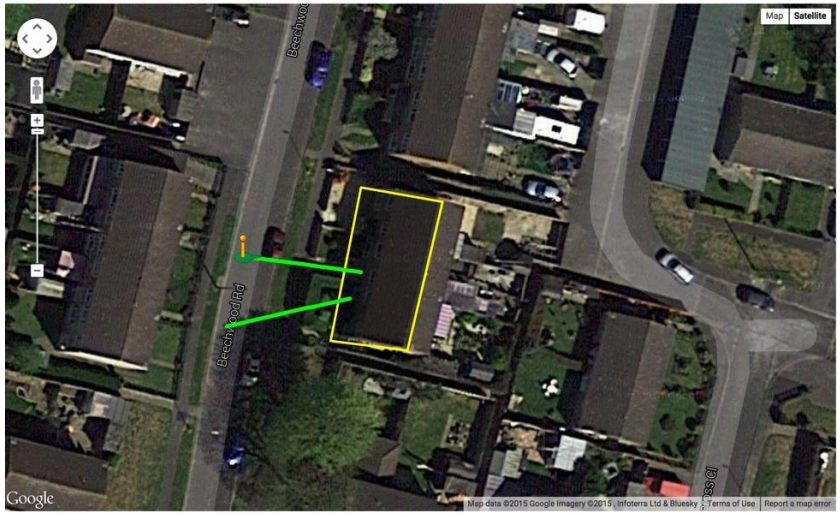
# COLLABMAP

In collaboration with Trung Dong Huynh

ORCHID

# How to Trust Crowd-Produced Data




What is the Quality of the Data, given the involvement of unknown participants?

# Trusting Information and People

"Big Data Analytics"

*"Provenance, on any menu, is a sign that the people cooking the food care about it. It signals that they are passionate about quality and have taken the time and effort to source their ingredients. (http://www.herald.ie/)*

- Network metrics:
  - summary of topological structure of provenance graphs
  - provenance metrics that are specific to provenance graphs
- Analytics applied to provenance
  - Predictive models of quality of data in crowd-sourced applications

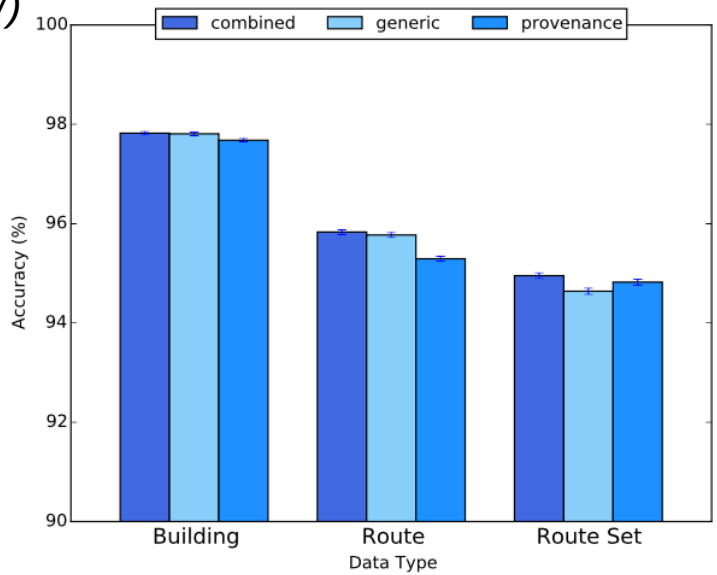



Figure 7. The accuracy of quality classifiers for CollabMap buildings, routes, and route sets learned from generic and/or provenance-specific network metrics.

Huynh, D. T., Ebden, M., Venanzi, M., Ramchurn, S. D., Roberts, S. J., & Moreau, L. (2013). Interpretation of Crowdsourced Activities Using Provenance Network Analysis. In The First AAAI Conference on Human Computation and Crowdsourcing.

**Highlight**.

Due diligence is the investigative process leading to informed decision making.

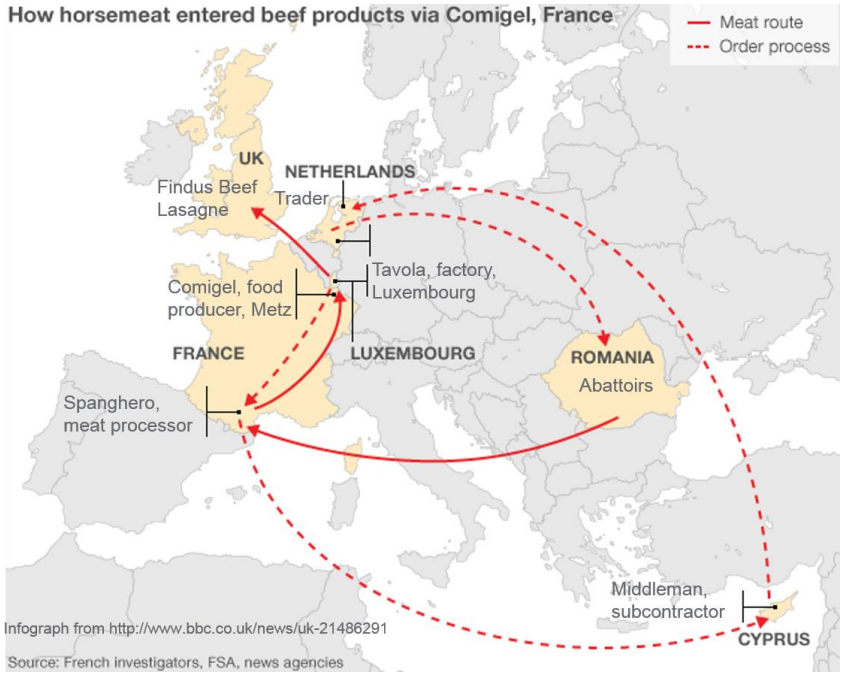
Provenance helps undertake and demonstrate due diligence.

# FOOD PROVENANCE

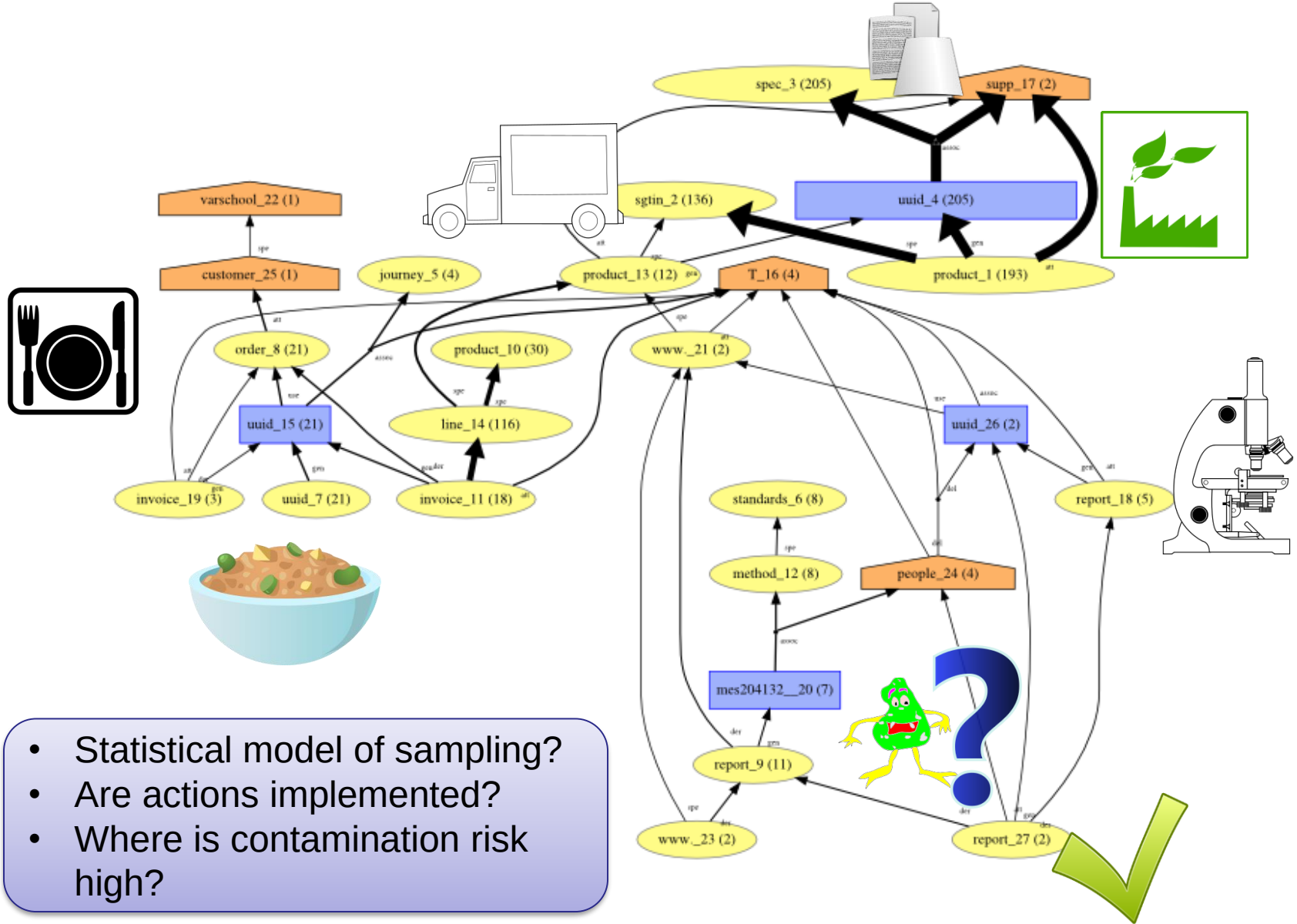
In collaboration with Belfrit Batlajery,Trung Dong Huynh, Danius Michaelides, Glenn Taylor, Alistair Sackley

# Provenance of Complex Supply Chains

- Context: the horse meat scandal
- General motivation: what is due diligence on the food chain
- Map the flows of orders, food products and financial flow
- Analytics: outliers, statistical models of sampling, checking of processes



# From Farms to School Meals



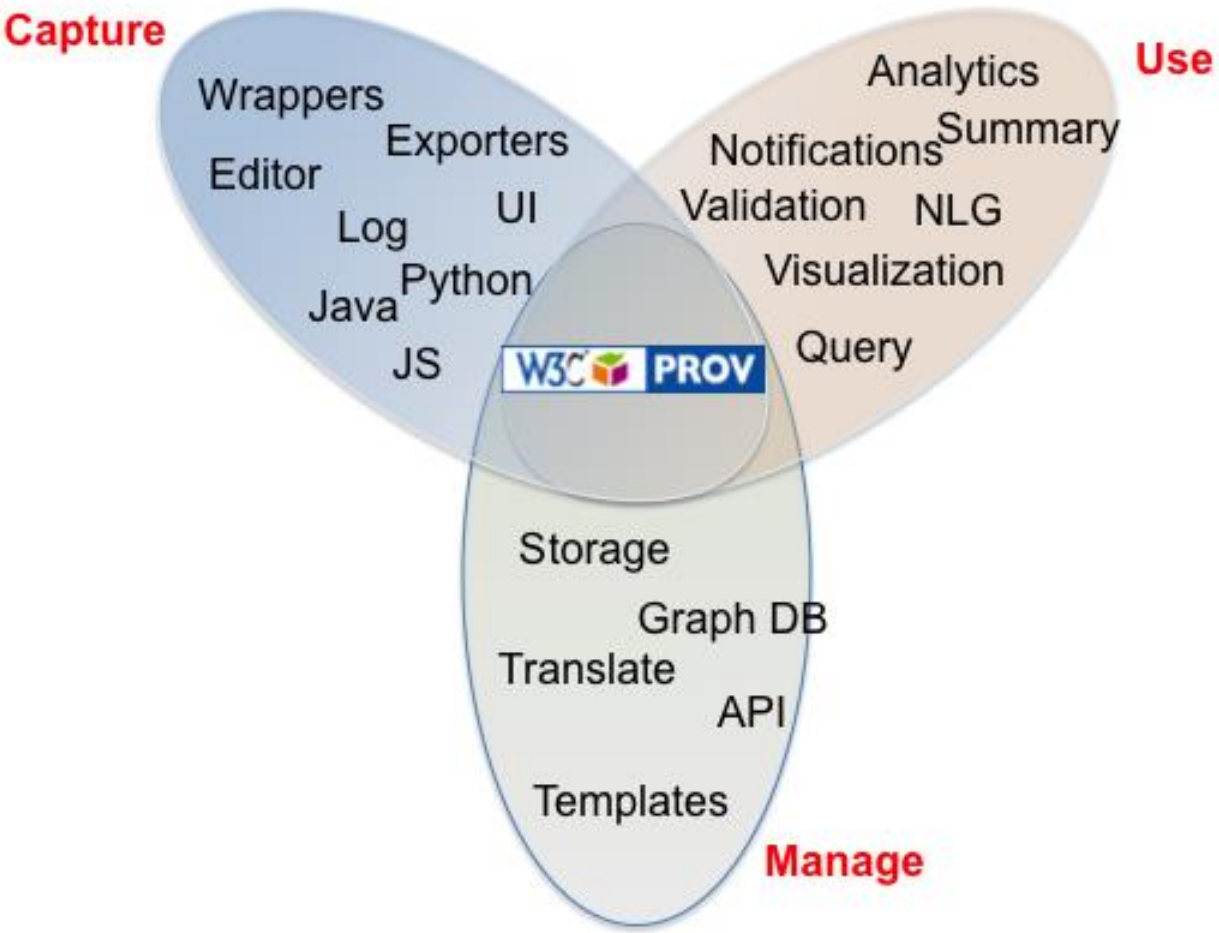

- Statistical model of sampling?
- Are actions implemented?
- Where is contamination risk high?

# Application Summary

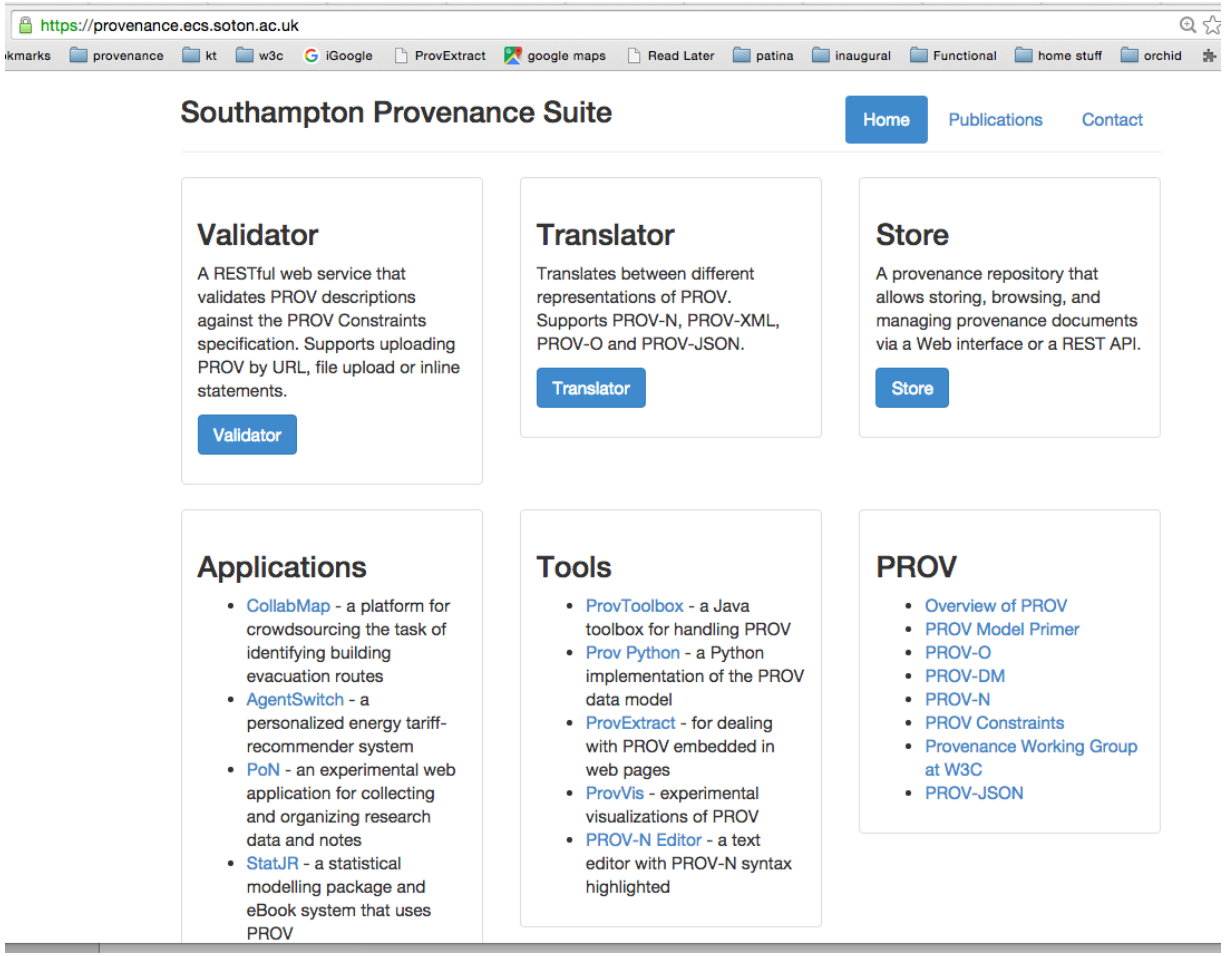
- Rideshare: provenance summarization
- Atomic Orchid: provenance notiifications
- Collabmap: predictive modelling
- Food Provenance: analytics
- Interactive Books: reproducibility
- PICASO: templates, linked data, influence

# INFRASTRUCTURE

# Software Infrastructure



# Software Infrastructure




https://provenance.ecs.soton.ac.uk

Provenance Management

Software Engineering and Provenance

Provenance and Distributed Ledger

Provenance for Humans

Provenance and Accountability

# NEW DIRECTIONS

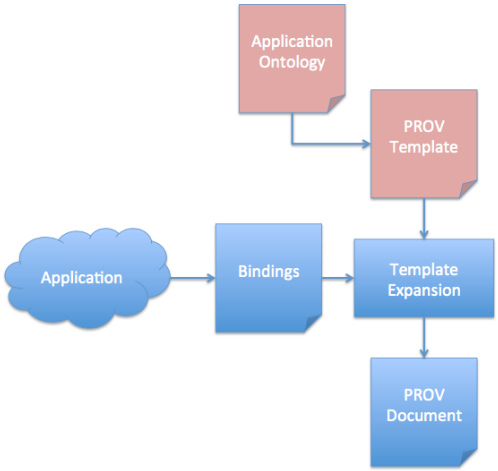
# Provenance Management

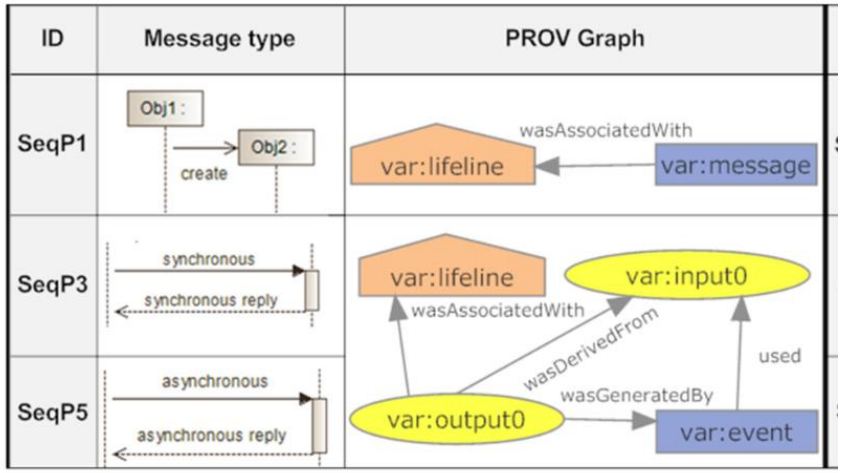
- Provenance Template
  - To create, store and query provenance
- Provenance Transformations
  - To abstract or refine provenance
  - To summarise provenance
  - To hide sensitive parts
- Provenance Analytics Pipeline
  - To ingest stream of provenance data
  - To process and analyse provenance

# Provenance and Software Engineering

Work with Carlos Saenz Adan and Beatriz Pérez Valle

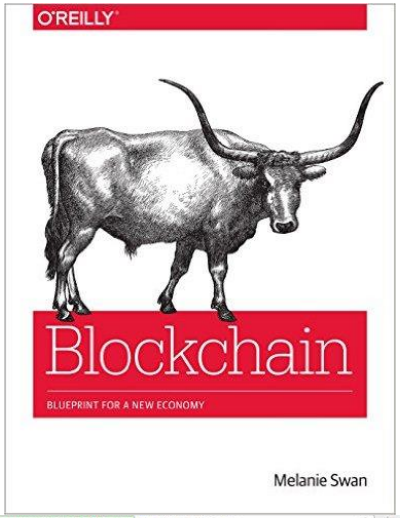
- How do we integrate "provenance management" in the software engineering lifecycle?
- From UML to provenance
- Outstanding issues: REST management, storage, …

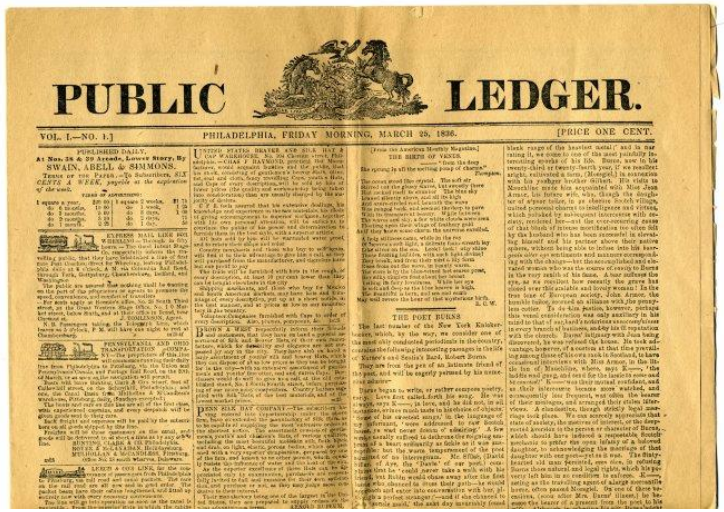


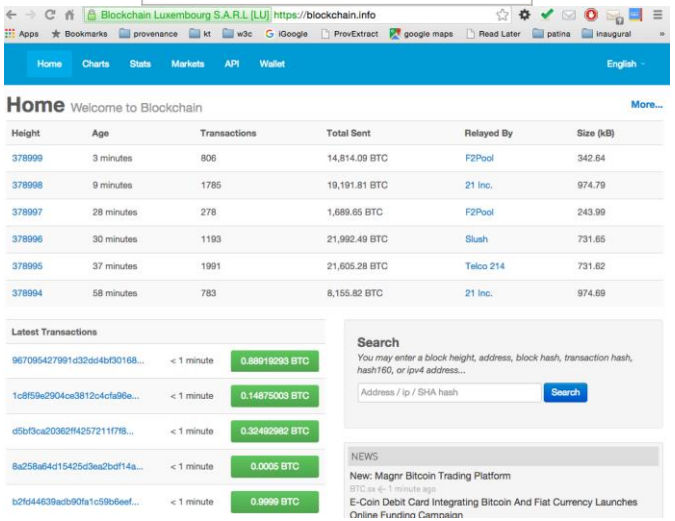



# Public ledgers & Provenance

- Block chain technology offers unforgeable public ledger
- Combine private/public provenance with public ledgers to make provenance trustable
- Doesn't have to be on Bitcoin's blockchain, but could be hosted on trusted host.

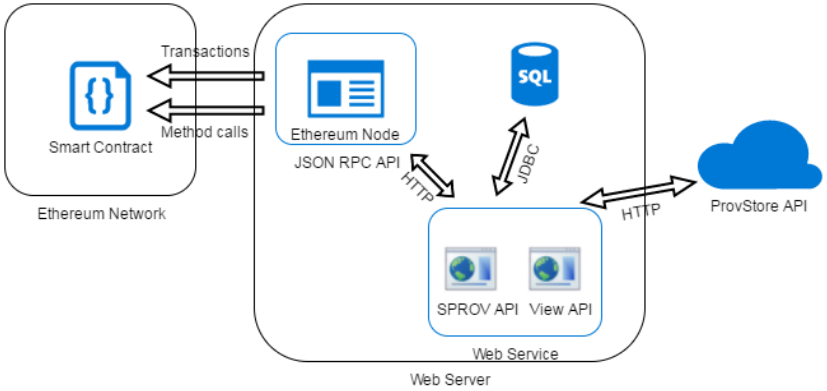


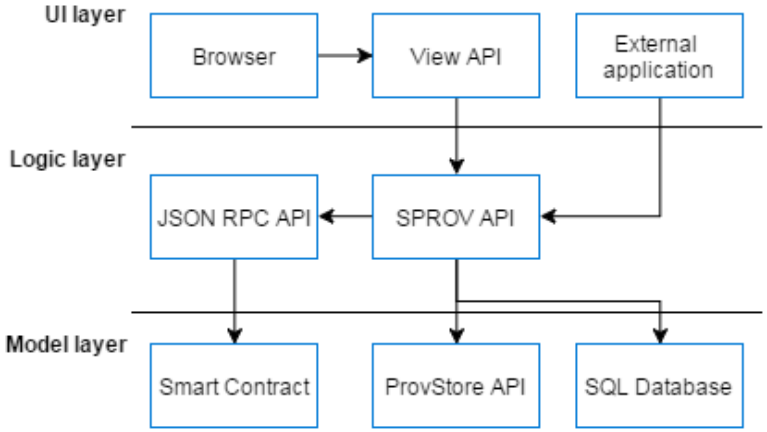



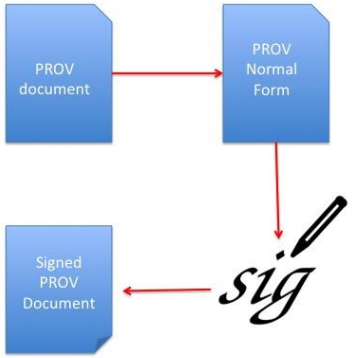
# ProvStore & Ethereum

Work with Ivaylo Varbanov

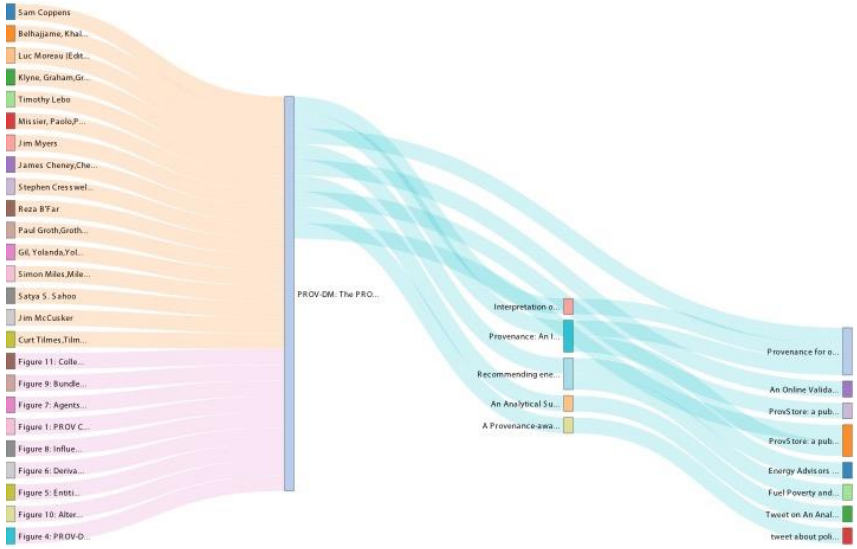


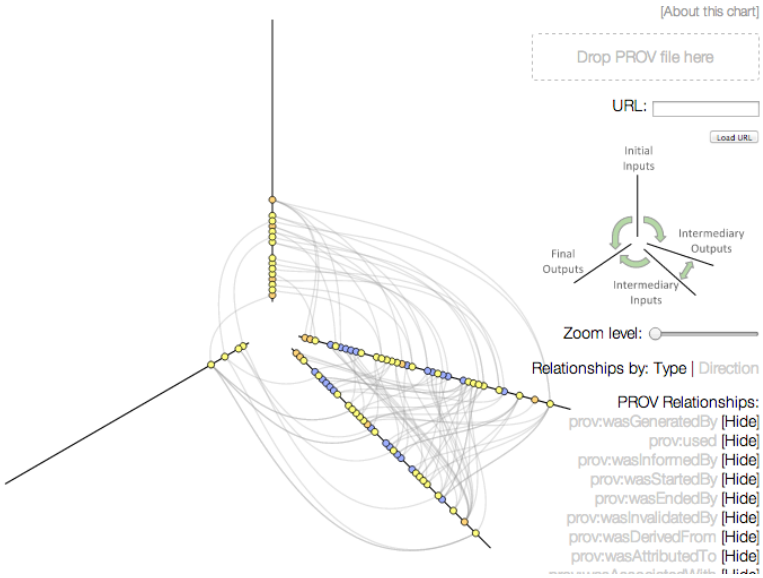

- Signed PROV documents
- Store PROV document in ProvStore
- Store signature in Ethereum



# Provenance for Humans: Visualization

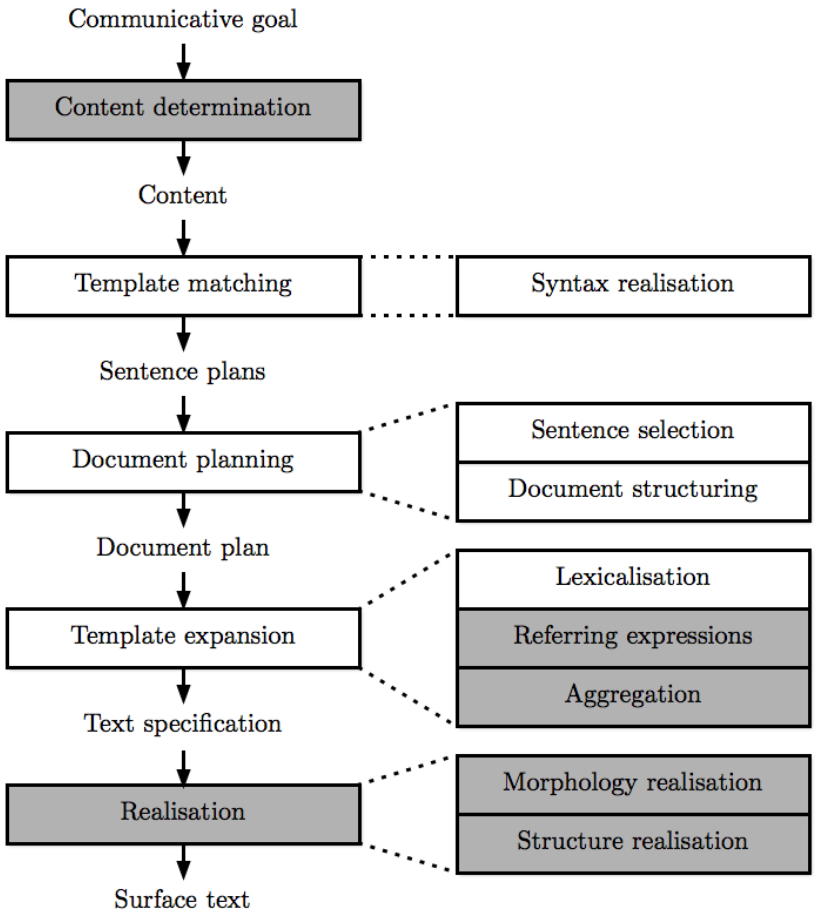


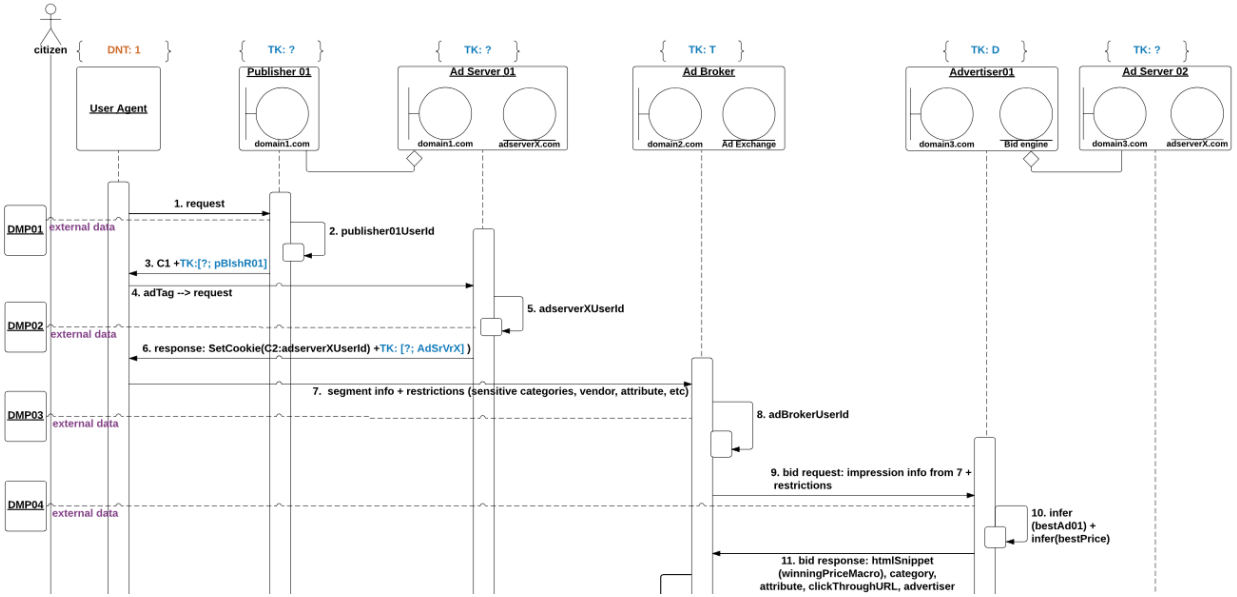
# Provenance for Humans: NLG

Work with Darren Richardson

- Users increasingly *choosing* to communicate with their devices verbally, in natural language (e.g. Siri)
- Text-to-speech and capabilities now good enough
- Conversion of PROV to text gives verbal communication
- Challenge: **Transform PROV graphs into text intelligible to a casual user**
- **Where can we get the linguistic information to perform this transformation?**
- **URIs**: as per RFC, contain no linguistic information, but in practice contain useful information



# Accountability in Online Behavioural Advertising




with
Faranak Hardcastle
and
Susan Halford

- Why was this advert targeted to me?
- Which advertisers? Which broker?
- Which profile of me do they have?

# Conclusions

- Provenance is crucial to make systems accountable
- Standard leads to impact beyond research community
- Automated processing over provenance allow for powerful instrospection capabilities
- Key issues going forward:
  - Analytics over provenance
  - Provenance management in the SE lifecycle
  - Communicating provenance to humans
  - Signatures, distributed ledgers
  - Foundations of accountability