Can Christopher eat it?
- or Semantics, Block chains and Ricardian Contracts

Christopher Brewster - TNO
based on conversations with
Vinay Gupta - Consensys/Ethereum

The Problem

- In a world of the Virtual Tomato, **how do I know it is organic**?
- or that dish x is vegetarian?
- or kosher/halal etc.?
- Let's call this **Christopher's digital predicament**

Currently …

- We rely on “trust” and “reputation”

- Brands and labels

- And we all know there is a lot of fraud and adulteration

Blockchains and trust

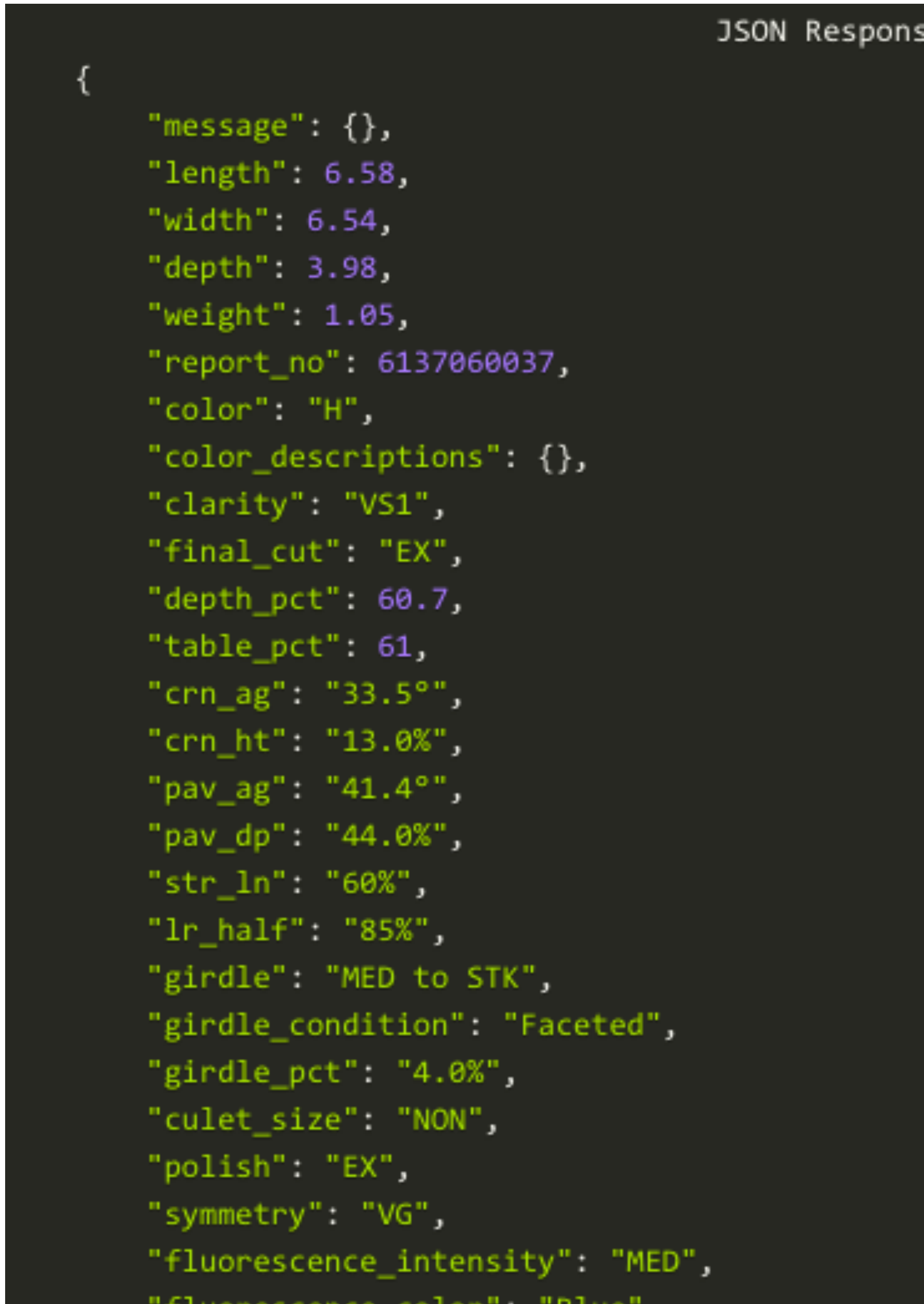
- One of the key supposed advantages is the need to remove third parties in transactions
- Simple example:
  - Bitcoin transaction occur without external third parties - no escrow
  - Basically a piece of digit information goes from location x to location y (where x and y are cryptographic GUIDs)
- Complex example:
  - My tomato is organic!
  - .errr ….

Blockchains and semantics

- This is really two problems:
    - Semantic/data structure - how to describe an “organic tomato”
    - Trust/validity - how to know this is true, how to know we mean the same thing
        - This closely related to the old AI problem called the “symbol grounding problem”

The need for semantics in blockchain technology

- Most current conceptions of blockchain use are:
  - either very narrow (e.g. provenance.org thinks of “is it certified or not”)
  - or quite arbitrary e.g. Ever ledger diamond description:
  - **There is an obvious need for ontologies here**



JSON Respons

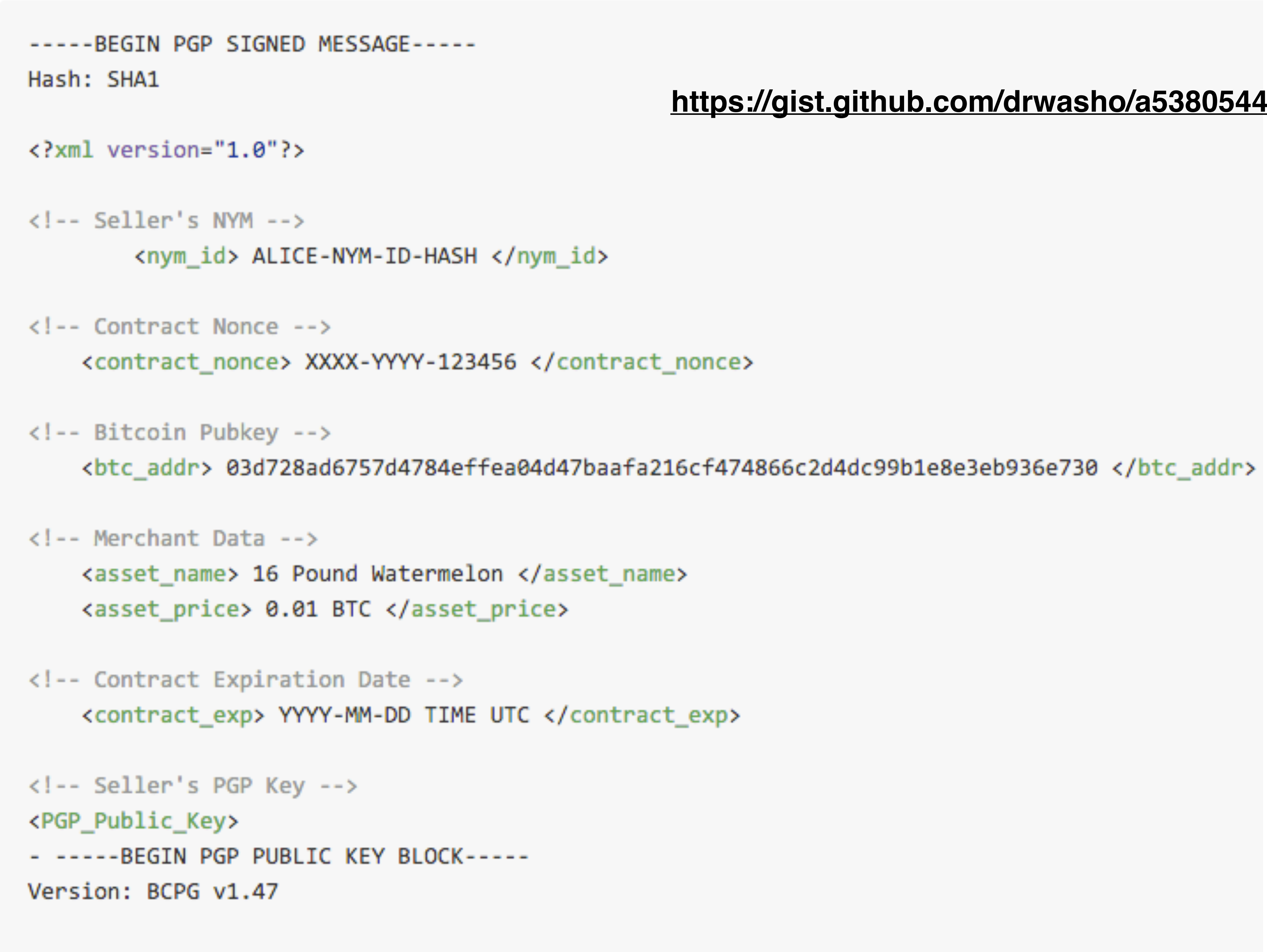
```
{
    "message": {},
    "length": 6.58,
    "width": 6.54,
    "depth": 3.98,
    "weight": 1.05,
    "report_no": 6137060037,
    "color": "H",
    "color_descriptions": {},
    "clarity": "VS1",
    "final_cut": "EX",
    "depth_pct": 60.7,
    "table_pct": 61,
    "crn_ag": "33.5°",
    "crn_ht": "13.0%",
    "pav_ag": "41.4°",
    "pav_dp": "44.0%",
    "str_ln": "60%",
    "lr_half": "85%",
    "girdle": "MED to STK",
    "girdle_condition": "Faceted",
    "girdle_pct": "4.0%",
    "culet_size": "NON",
    "polish": "EX",
    "symmetry": "VG",
    "fluorescence_intensity": "MED",
    "fluorescence_color": "Blue"
```

Ricardian Contracts

- **Ricardian contract** invented by Ian Grigg (specialist in financial cryptography)
- “A digital contract that defines the terms and conditions of an interaction, between two or more peers, that is cryptographically signed and verified”
- Importantly it is both **human and machine readable** and digitally signed
- “The ultimate test of our mission is if the legal profession can take a Ricardian contract and unambiguously decide points of dispute.” — Ian Grigg - **http://www.webfunds.org/guide/ricardian.html**
    - They have been tested in court successfully cf. DigiGold v. Systemics, before the Supreme Court of Anguilla (2001)

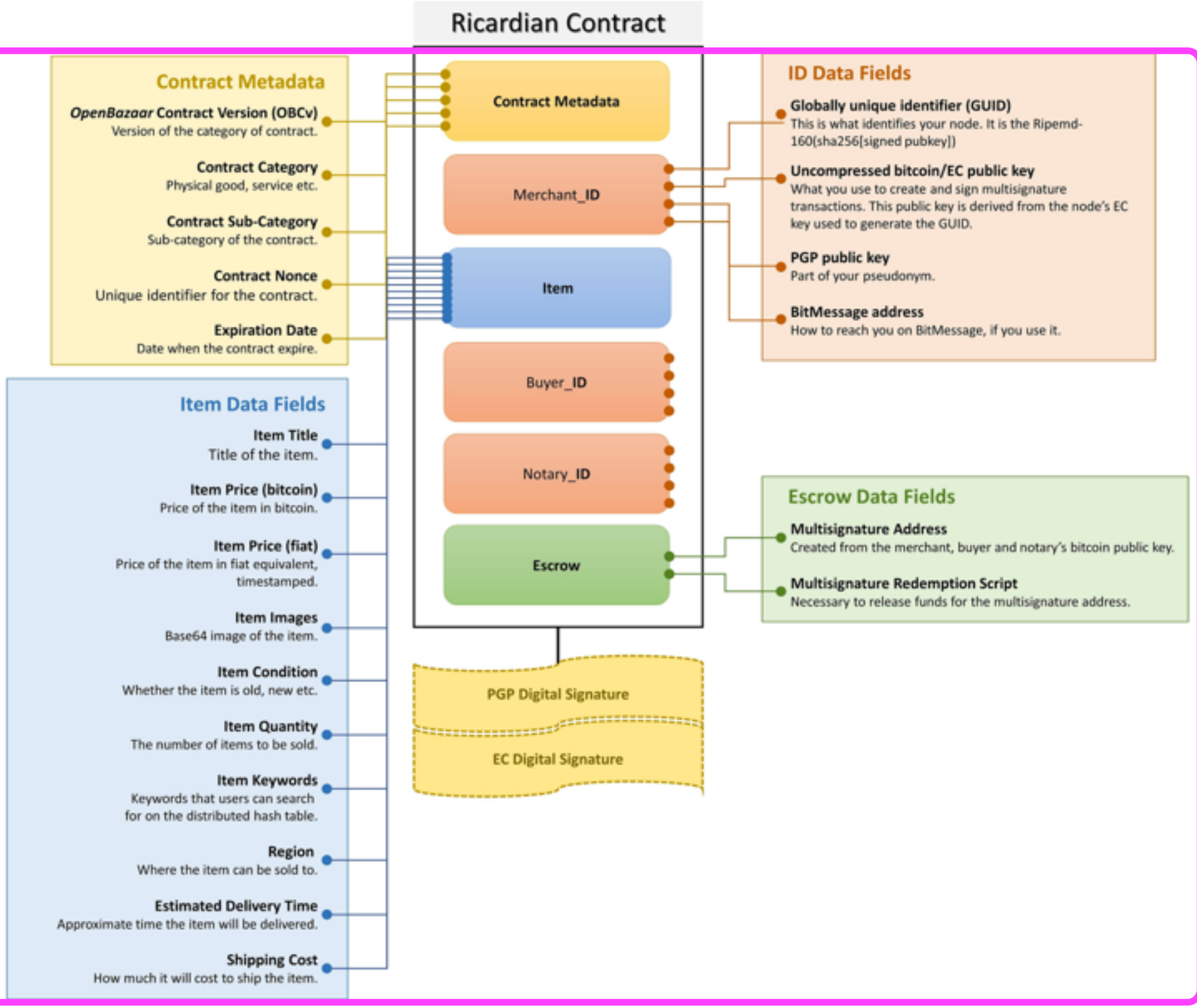
Example Ricardian contract - from OpenBazar

https://gist.github.com/drwasho/a5380544c170bdbbbad8#example



```
-----BEGIN PGP SIGNED MESSAGE-----
Hash: SHA1

<?xml version="1.0"?>

<!-- Seller's NYM -->
        <nym_id> ALICE-NYM-ID-HASH </nym_id>

<!-- Contract Nonce -->
    <contract_nonce> XXXX-YYYY-123456 </contract_nonce>

<!-- Bitcoin Pubkey -->
    <btc_addr> 03d728ad6757d4784effea04d47baafa216cf474866c2d4dc99b1e8e3eb936e730 </btc_addr>

<!-- Merchant Data -->
    <asset_name> 16 Pound Watermelon </asset_name>
    <asset_price> 0.01 BTC </asset_price>

<!-- Contract Expiration Date -->
    <contract_exp> YYYY-MM-DD TIME UTC </contract_exp>

<!-- Seller's PGP Key -->
<PGP_Public_Key>
- -----BEGIN PGP PUBLIC KEY BLOCK-----
Version: BCPG v1.47
```

Contract Schema



Ricardian Contract

Contract Metadata

Merchant_ID

Item

Buyer_ID

Notary_ID

Escrow

PGP Digital Signature

EC Digital Signature

Contract Metadata

OpenBazaar Contract Version (OBCv)
Version of the category of contract.

Contract Category
Physical good, service etc.

Contract Sub-Category
Sub-category of the contract.

Contract Nonce
Unique identifier for the contract.

Expiration Date
Date when the contract expire.

Item Data Fields

Item Title
Title of the item.

Item Price (bitcoin)
Price of the item in bitcoin.

Item Price (fiat)
Price of the item in fiat equivalent, timestamped.

Item Images
Base64 image of the item.

Item Condition
Whether the item is old, new etc.

Item Quantity
The number of items to be sold.

Item Keywords
Keywords that users can search for on the distributed hash table.

Region
Where the item can be sold to.

Estimated Delivery Time
Approximate time the item will be delivered.

Shipping Cost
How much it will cost to ship the item.

ID Data Fields

Globally unique identifier (GUID)
This is what identifies your node. It is the Ripemd-160(sha256[signed pubkey])

Uncompressed bitcoin/EC public key
What you use to create and sign multisignature transactions. This public key is derived from the node's EC key used to generate the GUID.

PGP public key
Part of your pseudonym.

BitMessage address
How to reach you on BitMessage, if you use it.

Escrow Data Fields

Multisignature Address
Created from the merchant, buyer and notary's bitcoin public key.

Multisignature Redemption Script
Necessary to release funds for the multisignature address.

Replace the contract with an ontology or include an ontology.

http://www.webfunds.org/guide/ricardian.html

Ontologies in the Ricardian Contracts

- Essentially transferring the symbol grounding problem to the law courts
- If you disagree on meaning of X, sue me!

Ricardian Contracts and Smart Contracts

- Ricardian contract human readable **and** machine readable - conceived as a set of attribute values

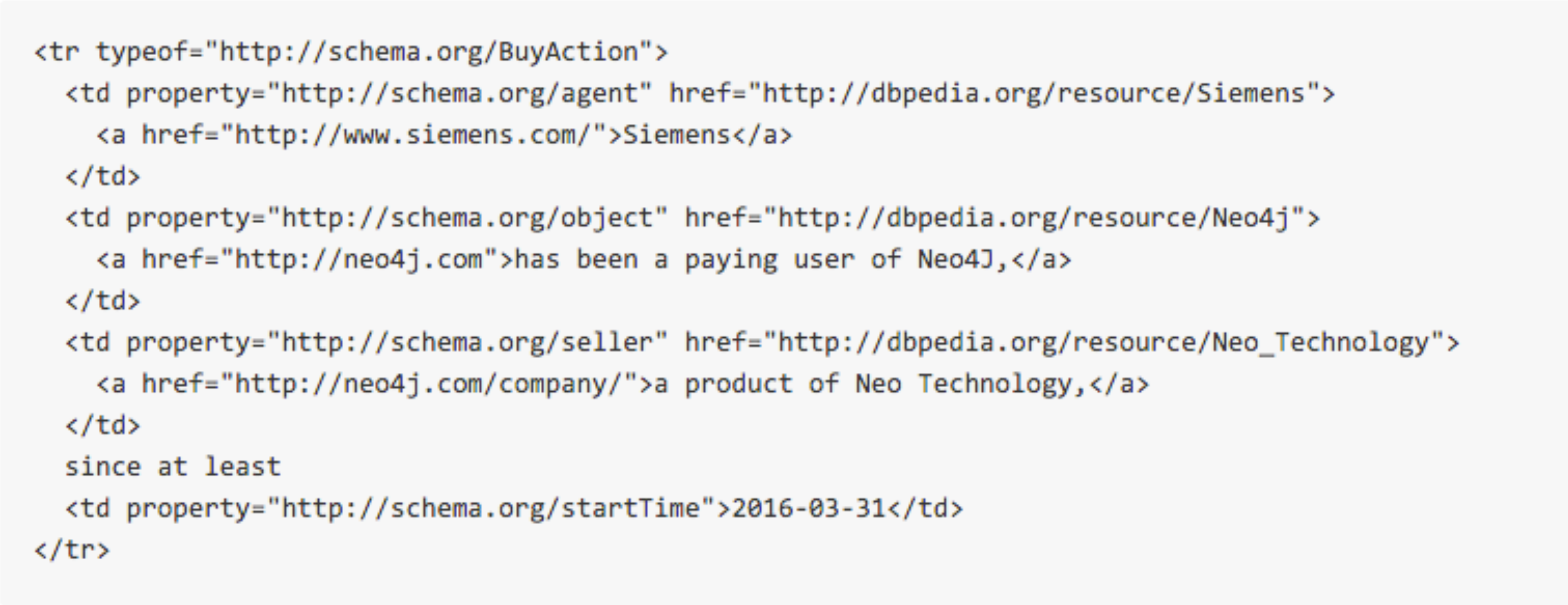
- Smart contract is a piece of code which executes — which may execute a Ricardian Contract

    - “the smart contract is really the machine to perform the contract” - Ian Grigg

Ontology Based Prediction Markets

- Blog post by Stefano Bertolo
  - Concerns Augur - an Ethereum based prediction market
  - Alice stablished a market for the prediction “"By March 31 2016, Siemens will have become a customer of Neo Technology”"
  - Basically suggests that one can use ontologies (in this case schema.org) to formalise the a. description of the prediction, b. the evaluation of the correctness

Formal representation of a prediction



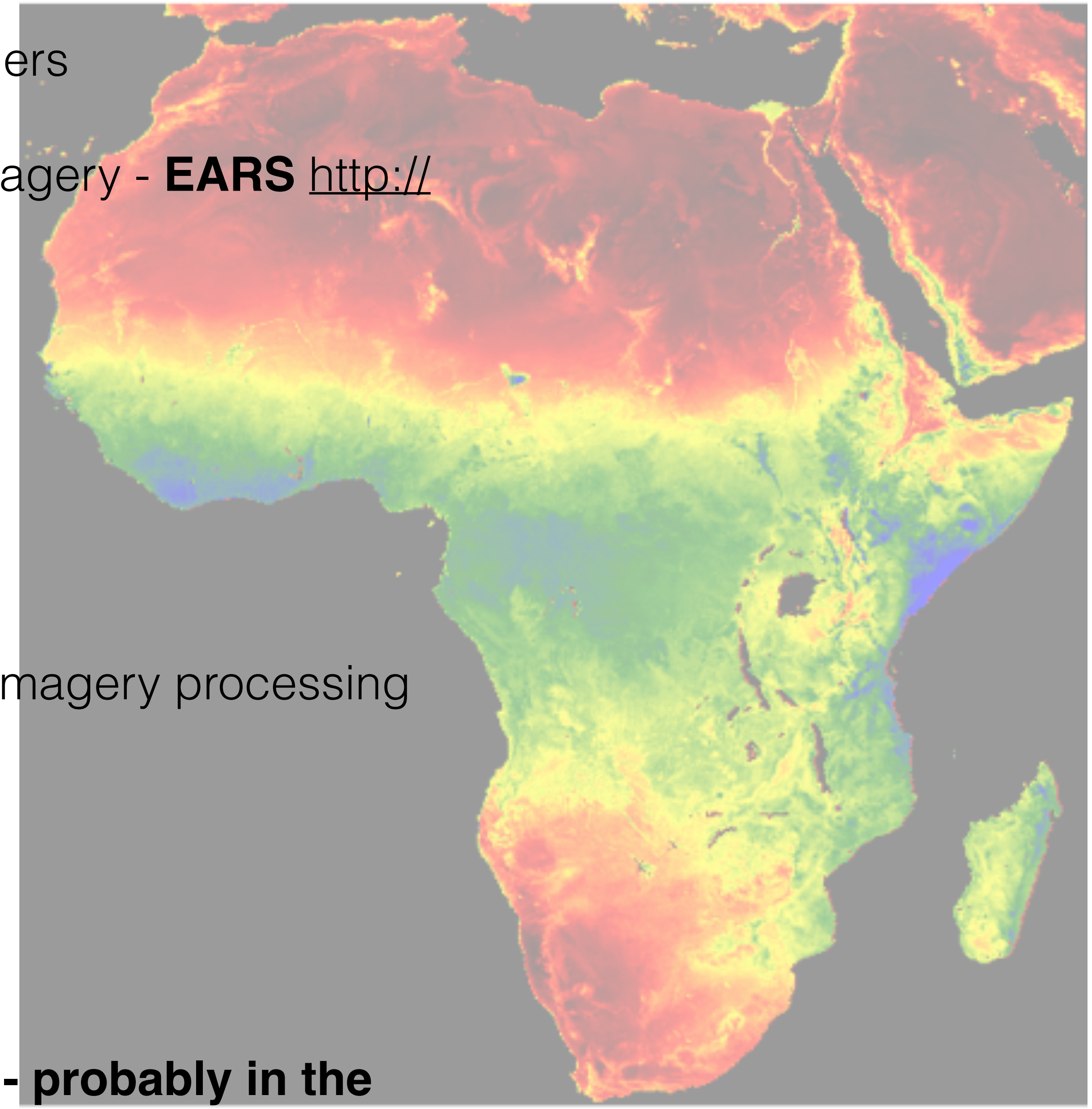
```
<tr typeof="http://schema.org/BuyAction">
  <td property="http://schema.org/agent" href="http://dbpedia.org/resource/Siemens">
    <a href="http://www.siemens.com/">Siemens</a>
  </td>
  <td property="http://schema.org/object" href="http://dbpedia.org/resource/Neo4j">
    <a href="http://neo4j.com">has been a paying user of Neo4J,</a>
  </td>
  <td property="http://schema.org/seller" href="http://dbpedia.org/resource/Neo_Technology">
    <a href="http://neo4j.com/company/">a product of Neo Technology,</a>
  </td>
  since at least
  <td property="http://schema.org/startTime">2016-03-31</td>
</tr>
```

https://github.com/sclopit/essays/blob/master/ontopreds.md

Resolving the prediction

- Bertolo assumes triple stores exist which collect facts such as "On March 28, 2016 Siemens announced that it deploying Neo4J through a contract serviced by Neo Technology” as **triples**
- Then SPARQL queries are written against this data set
- Who is doing this: ThomsonReuters, New York Times, BBC, Ontotext, Google etc.
- Digital to physical interface crossed via news reports i.e. symbol grounding is via human interpretation and writing about events.

Agricultural Insurance scenario



- Let us imagine cheap crop insurance for African farmers
  - Already exists - Dutch company using satellite imagery - **EARS** http://www.ears.nl/
- Let us use Blockchains to:
  - collect insurance payments via a cryptocurrency
  - define Ricardian contracts for payout
  - define Smart contracts which undertake satellite imagery processing to determine payout
  - payout is returned as cryptocurrency
- Complete automation of every step
- **But only possible if every step is formally defined - probably in the form of ontologies**

Organic Tomatoes (again)

- Requirements:
  - Use **ontologies** to represent the tomato and the organic food attributes formally
  - Use **Ricardian Contracts** to legally guarantee truth and validity with **ontologies** embedded
  - Use **smart contracts** to test if food is organic or not (????)
- ***May be possible using continuous sensors attached to plants testing bio-electric potential over time!*** *cf the PLEASED project http://www.fastcoexist.com/3025753/using-plants-as-sensors-to-create-a-global-monitoring-system* ***or*** *the iPhone app http://www.fastcodesign.com/1670479/iphone-sensors-test-if-your-food-really-is-organic*

Questions?
Suggestions!

Further reading/links

- http://iang.org/papers/ricardian_contract.html
- http://www.webfunds.org/guide/ricardian_implementations.html
- http://www.everledger.io/
- https://en.wikipedia.org/wiki/Symbol_grounding_problem
- https://blog.openbazaar.org/decentralized-reputation-in-openbazaar/
- https://docs.google.com/document/d/1WgAoioqbV8JUNOmHVFo16D88e59mVj2SzFpFg2jmBx4/edit
- http://reliefweb.int/report/world/fesa-micro-insurance-crop-insurance-reaching-every-farmer-africa
- http://www.fastcoexist.com/3025753/using-plants-as-sensors-to-create-a-global-monitoring-system

Acknowledgements

- Images from Flickr:
    - https://c2.staticflickr.com/8/7142/6797712293_c09131a590_b.jpg
    - https://c1.staticflickr.com/5/4125/5106145638_85832d5135_b.jpg
    - https://c2.staticflickr.com/2/1209/1064944536_cfbaa5caa1_o.jpg