



# SEMANTIC BLOCKCHAIN REQUIREMENTS

Mentor:  
Prof. Dr. Maria-Esther Vidal

Team Members:  
Firas, Ernane, Matthew


# 1. Semantically describe the properties of a transaction



Functional

# What properties to describe ?

- ▶ Define or reuse a vocabulary of semantic concepts for transactions and their properties.
- ▶ Add additional Concepts to the vocabulary.
- ▶ Allow using internal vocabulary.



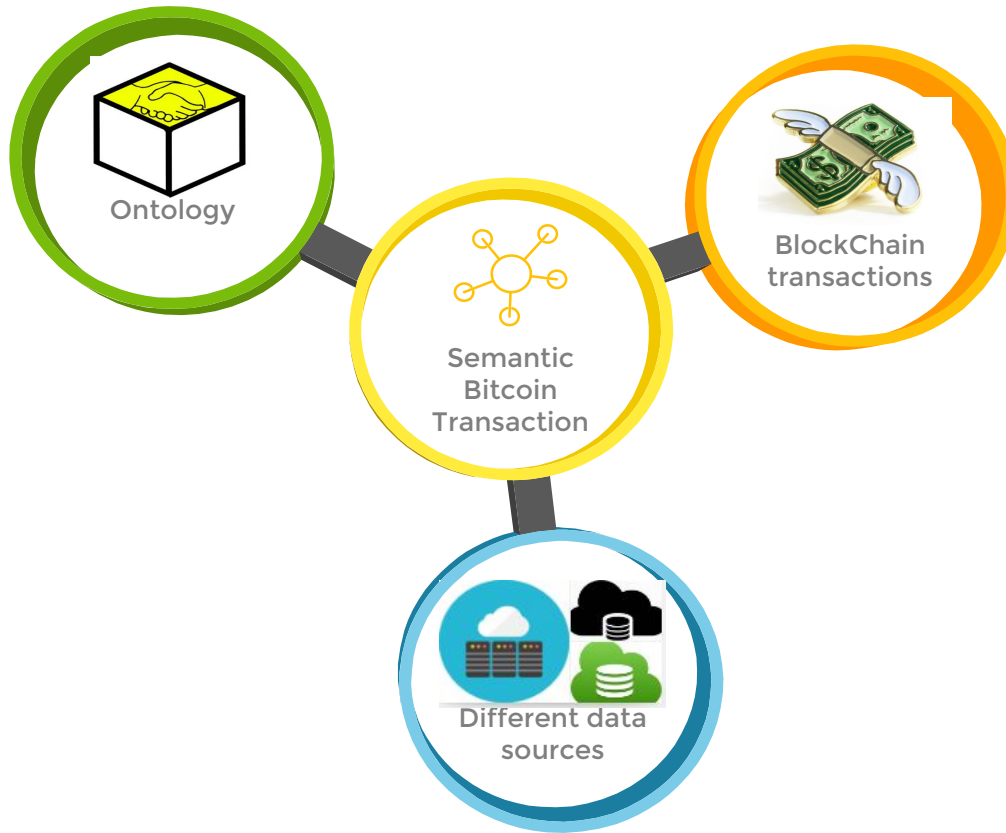
tx format version - currently at version 1

in-counter - number of input amounts

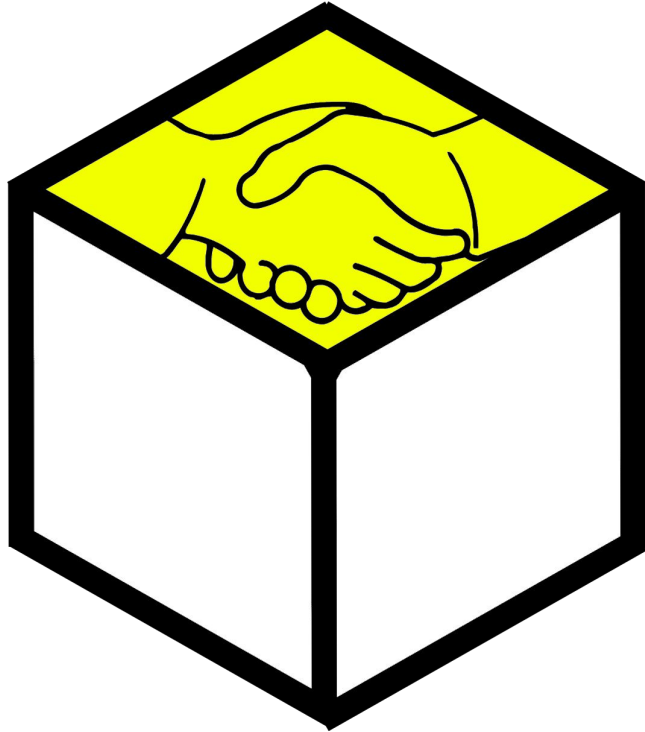
out-counter - number of output amounts

tx lock\_time - should be 0 or in the past  
for the tx to be valid and  
included in a block

size - of the transaction in bytes



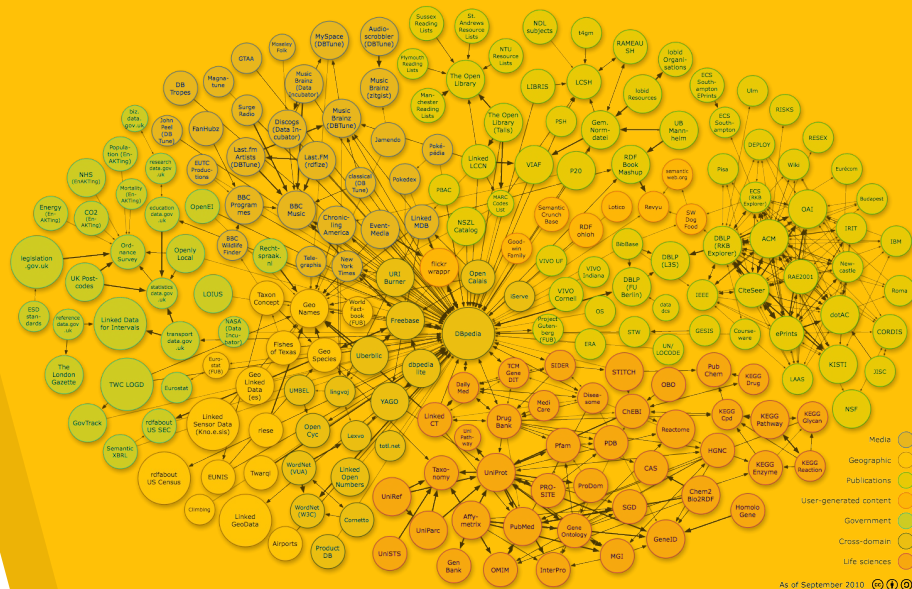
- Potential working ontology:



**BLONDIE**  
Blockchain  
Ontology with  
Dynamic Extensibility

# 2.

## Link to other data sources





## LINKED DATA



- ▶ Imagine you have one of the bitcoin addresses of Bill Gates

You can link that with his FOAF triples: [http://dbpedia.org/page/Bill\\_Gates](http://dbpedia.org/page/Bill_Gates)

- ▶ We can create a FOAF of satoshi and link it with his transactions:

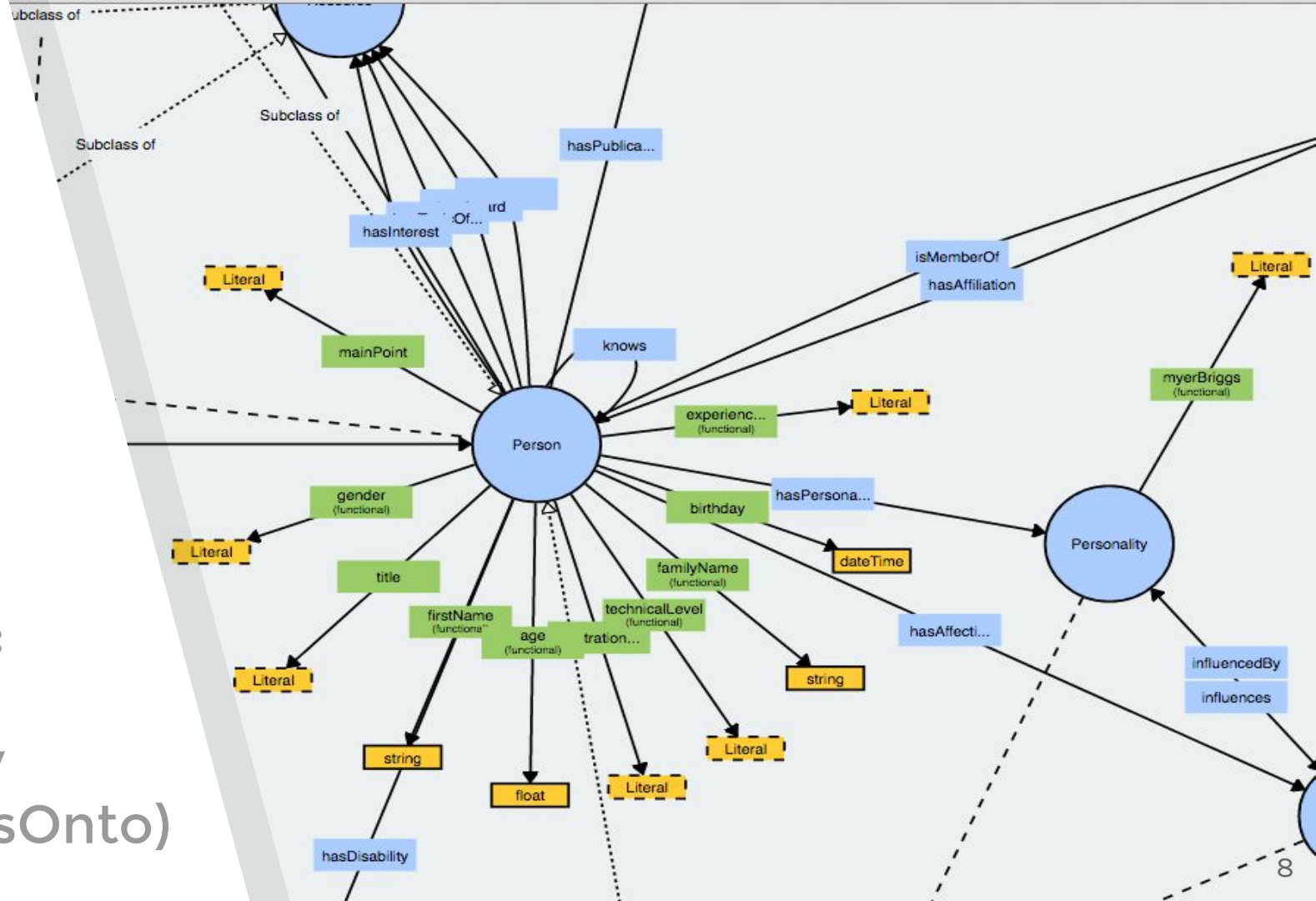
<http://www.theopenledger.com/9-most-famous-bitcoin-addresses/>

- ▶ Try to find who are all this guys:

<http://www.bitcoinrichlist.com/top100>

- ▶ Link those bitcoin addresses to their institutions triples [https://en.bitcoin.it/wiki/Donation-accepting\\_organizations\\_and\\_projects](https://en.bitcoin.it/wiki/Donation-accepting_organizations_and_projects)

# Example: Personas Ontology (PersonasOnto)





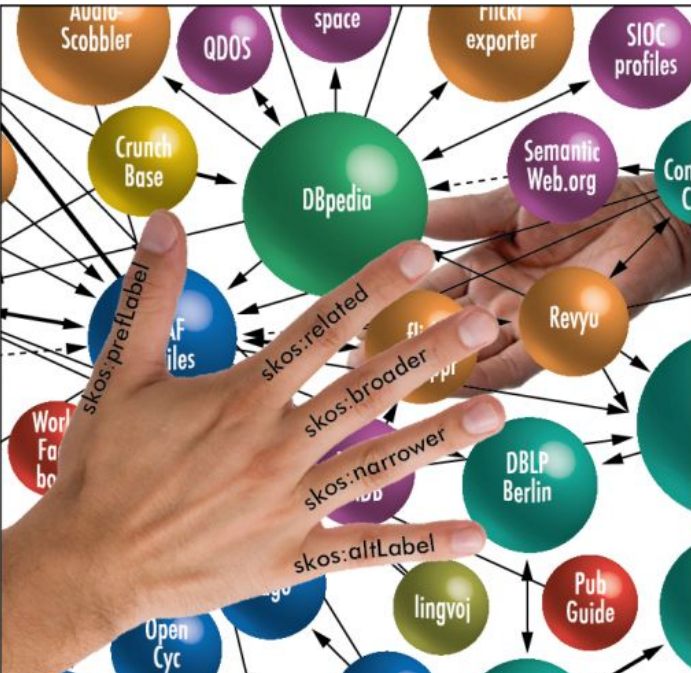


# Silk: The Linked Data Integration Framework

- ▶ Generating links between related data items within different Linked Data sources.
- ▶ Linked Data publishers can use Silk to set RDF links from their data sources to **other data sources** on the Web.
- ▶ Applying data transformations to structured data sources.

<http://silkframework.org/>

# 3. Semantic Data Management Techniques





**1. Provide local on the fly processing of transactions**



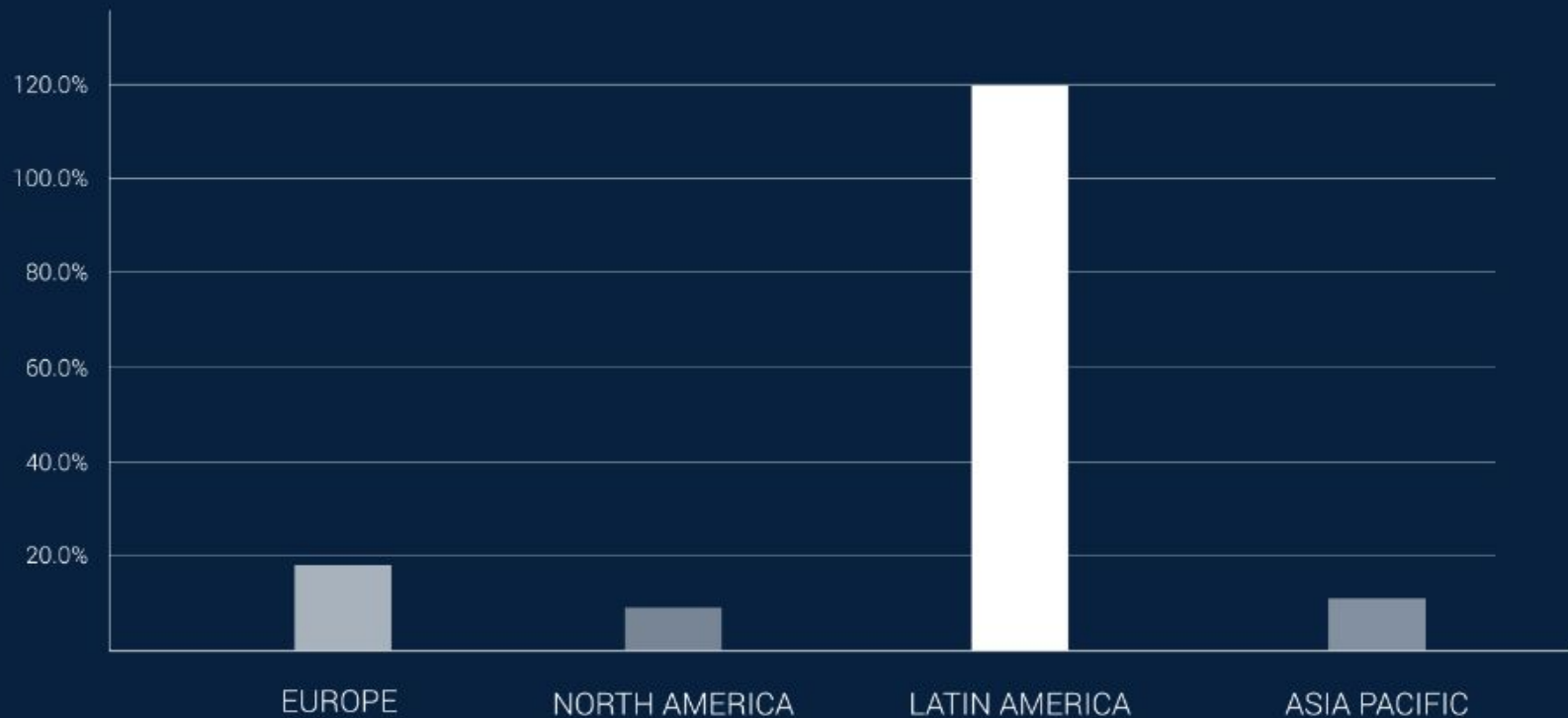
**2. Provide search and track operations on transactions.**

**3. Provide reports of transactions with a chosen criteria**



## TRANSACTION VOLUME GROWTH

Q1 -Q2 2015

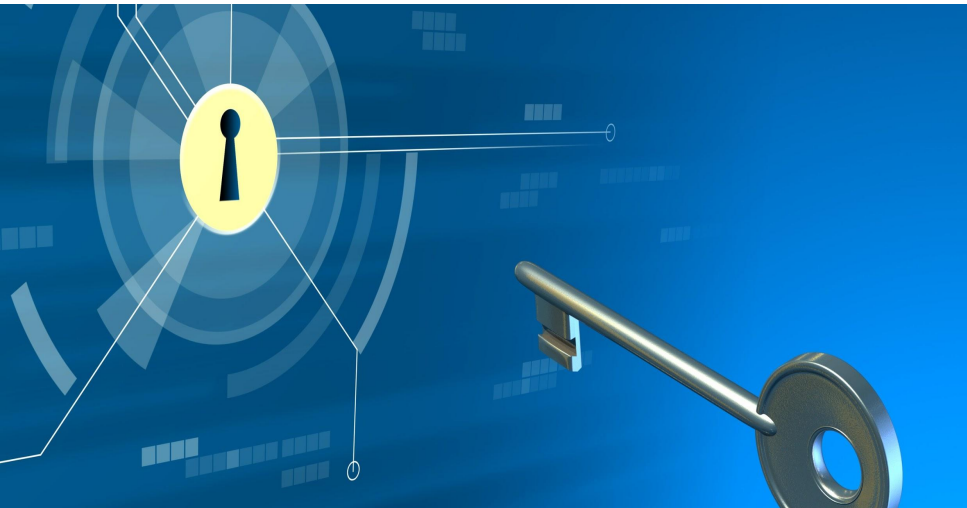


# The Balance report

Date	Destination	Note	Amount In	Amount Out	Gain/Loss	Balance
05/21/13	Coinbase: My Wall	Bought 0.4000 BT	0.4			0.4
05/29/13	1885WH4iZ3tMYfM			-0.4	2.07	0
06/04/13	Coinbase: My Wall	Bought 1.0000 BT	1			1
06/11/13	1885WH4iZ3tMYfM			-1	-16.34	0
06/20/13	Coinbase: My Wall	Bought 1.0000 BT	1			1
07/08/13	Coinbase: My Wall	Bought 2.0000 BT	2			3
07/12/13	Coinbase: My Wall	Bought 5.0000 BT	5			8
07/13/13	1JnVZNEE8Cs2Q4			-0.5	-11.67	7.5
07/19/13	My Wallet		0.279			7.779
07/28/13	Coinbase: My Wall	Bought 5.0000 BT	5			12.779
07/30/13	Sold to Coinbase	Sold 1.0000 BTC f		-1	-1.86	11.779
08/14/13	Sold to Coinbase	Sold 1.0000 BTC f		-1	20.98	10.779
08/19/13	Coinbase: My Wall	Bought 10.0000 B	10			20.779
08/19/13	166JJXva4QrjqG4f			-3	50.76	17.779
08/22/13	Coinbase: My Wall	Bought 3.0000 BT	3			20.779
09/08/13	1HRMnGyn5VVT2e			-0.5	13.41	20.279
09/08/13	18avApdunqqksZz			-3	86.15	17.279
09/08/13	My Wallet		3.71764405			20.99664405

# 4.

## Access control



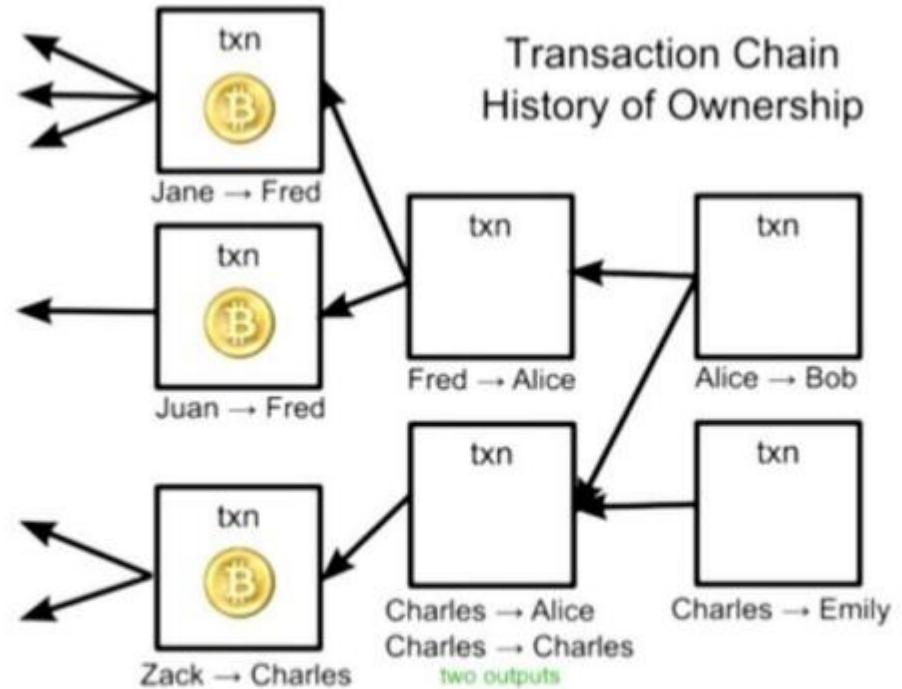


## Access Control and Privacy

- Create Access control to the inner vocabulary.
- Strict focus on (*exclusively*) public information.

Ignoring private information:

- ▶ Location of an address
- ▶ IP
- ▶ Wallet information

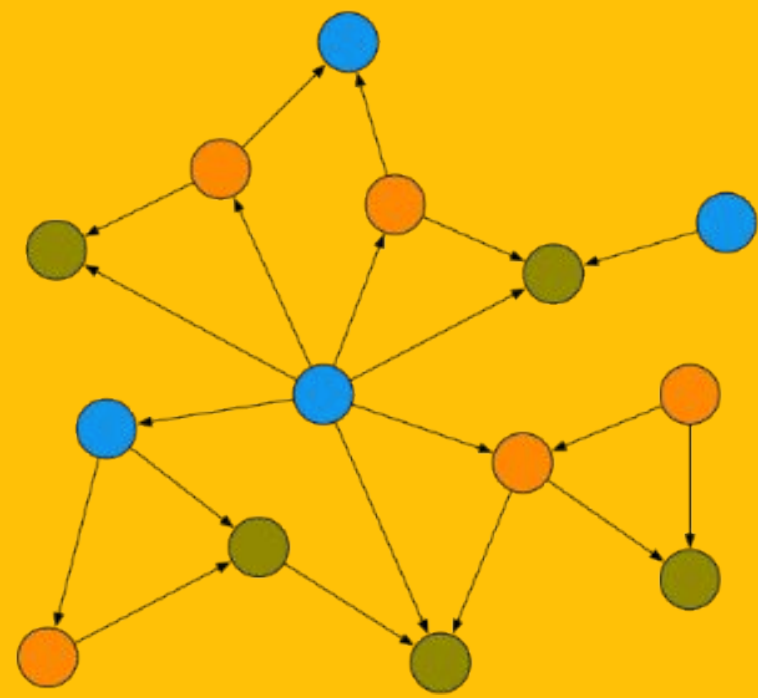
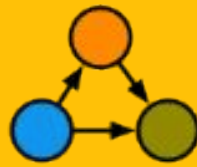


**Every single bitcoin can be traced to the start**

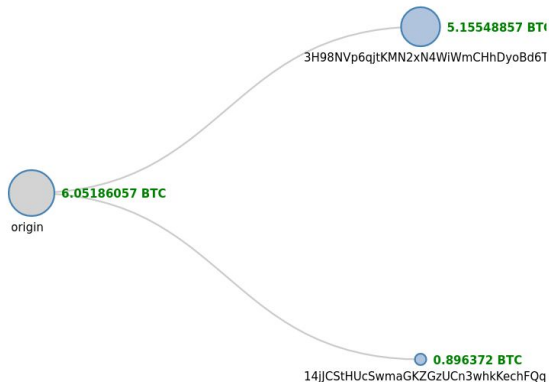


# 5.

## Application Domain



- Related to *'Ego-net community mining applied to friend suggestion'*



# Subgraph Mining

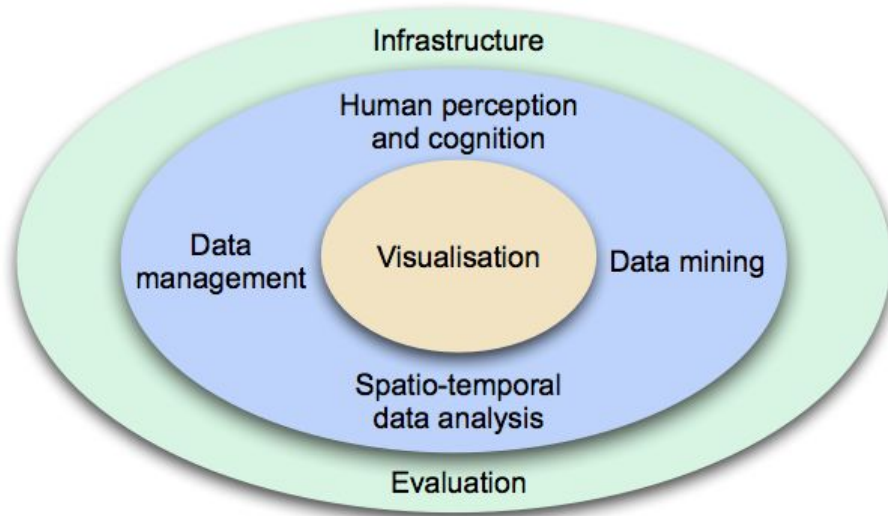
# 6.

## Enhanced Usability



# Provide Visualization

- To facilitate visual analysis and reduced cognitive load



# Non-functional requirements

1. **Performance.**
2. **Provide a User friendly visualization.**
3. **Process data on the fly.**
4. **Security**(ignoring private information).
5. **Availability** (Redundancy).
6. **User friendly transaction reports.**

# SEMANTIC BLOCKCHAIN

