Strategies for Integrating Semantic and Blockchain Technologies

DONE BY:

Héctor E. Ugarte R.

Msc. Computer Science

Semantic blockchain

Motivation


Martin Hiesboeck
6 April 2016

DIGITAL DOUGHNUT

Blockchain is the most disruptive invention since the Internet itself - not just in finance


theguardian

fashion environment te

Is Blockchain the most important IT invention of our age?

John Naughton


THE WALL STREET JOURNAL.

Going Mainstream

The World Economic Forum asked more than 800 executives and technology experts when they thought various tipping points would occur—when various technologies would hit mainstream society. Here are the respondents' expectations for two tipping points for blockchain technology.

ECONOMIC ROLE

TIPPING POINT: 10% of global gross domestic product stored on blockchain technology

AVERAGE EXPECTED DATE: 2027

"Bitcoin is a remarkable cryptographic achievement and the ability to create something that is not duplicable in the digital world has enormous value"

Eric Schmidt, CEO of Google

"I think the fact that within the bitcoin universe an algorithm replaces the functions of [the government] ... is actually pretty cool. I am a big fan of Bitcoin."

Al Gore, 45th Vice President of the United States

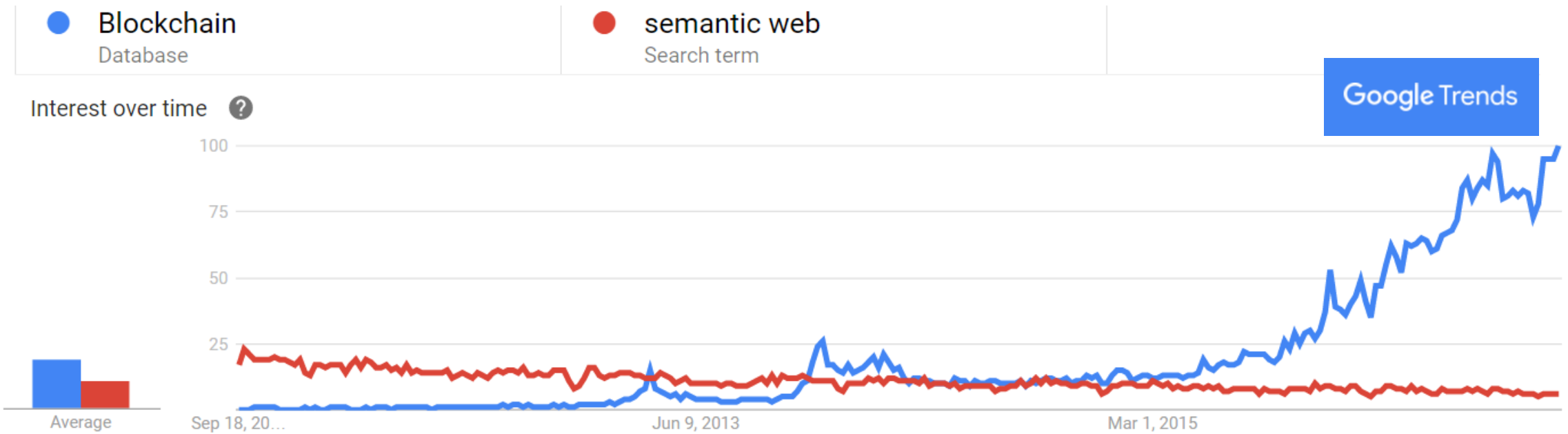
THE WALL STREET JOURNAL.

Subscribe Now | JOIN NOW

Why Blockchains Could Transform How the Economy Works

By IRVING WLADAWSKY-BERGER
Nov 20, 2015 1:27 pm ET

0 COMMENTS

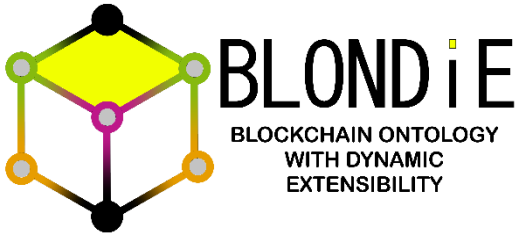


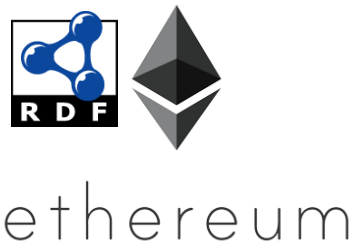
Problem definition

- Blockchain-based platforms as the original Web, still require interconnected data and meaning.
- Bitcoin: around 215,000 daily transactions.
- Ethereum: around 57,000 daily transactions.
- Existing Supply chain systems are not doing an optimal job, Blockchain-based platforms can solve this issue.

Solution proposed

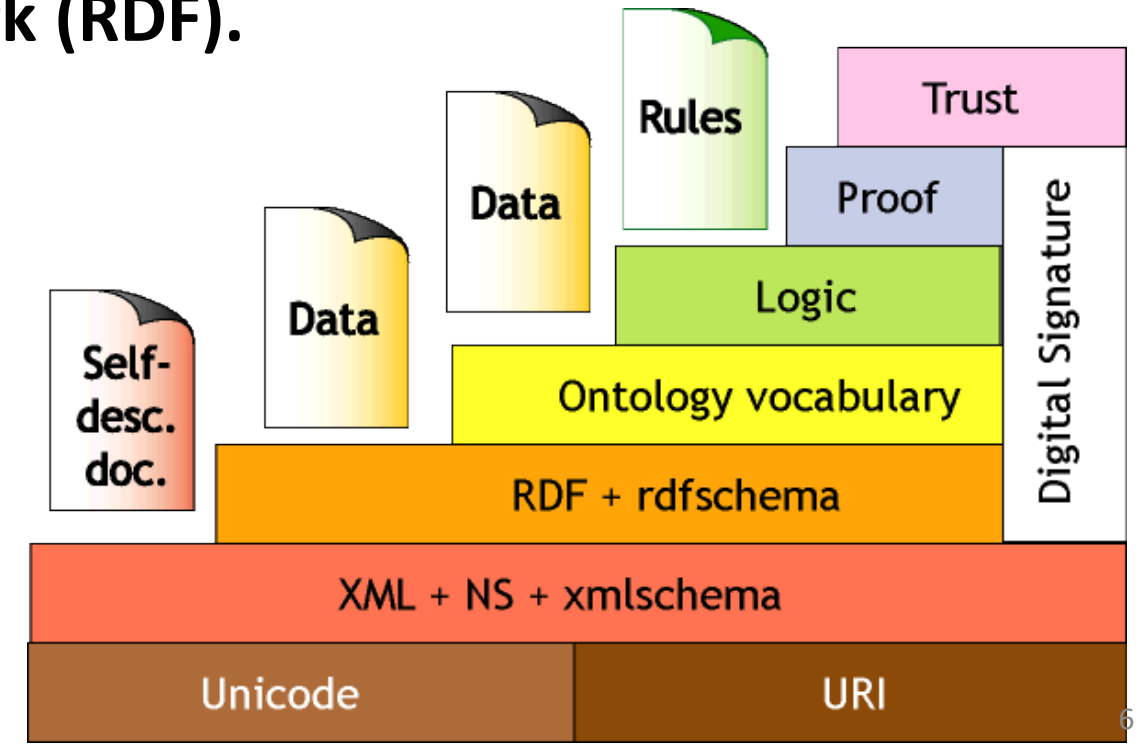
- Ontology BLONDiE for Bitcoin and Ethereum.
- Research how to extract data from Ethereum.
- Research how to store RDF data on Ethereum.
- Prototype DeSCA: Ethereum application.





Background: What is **Semantic Web?**

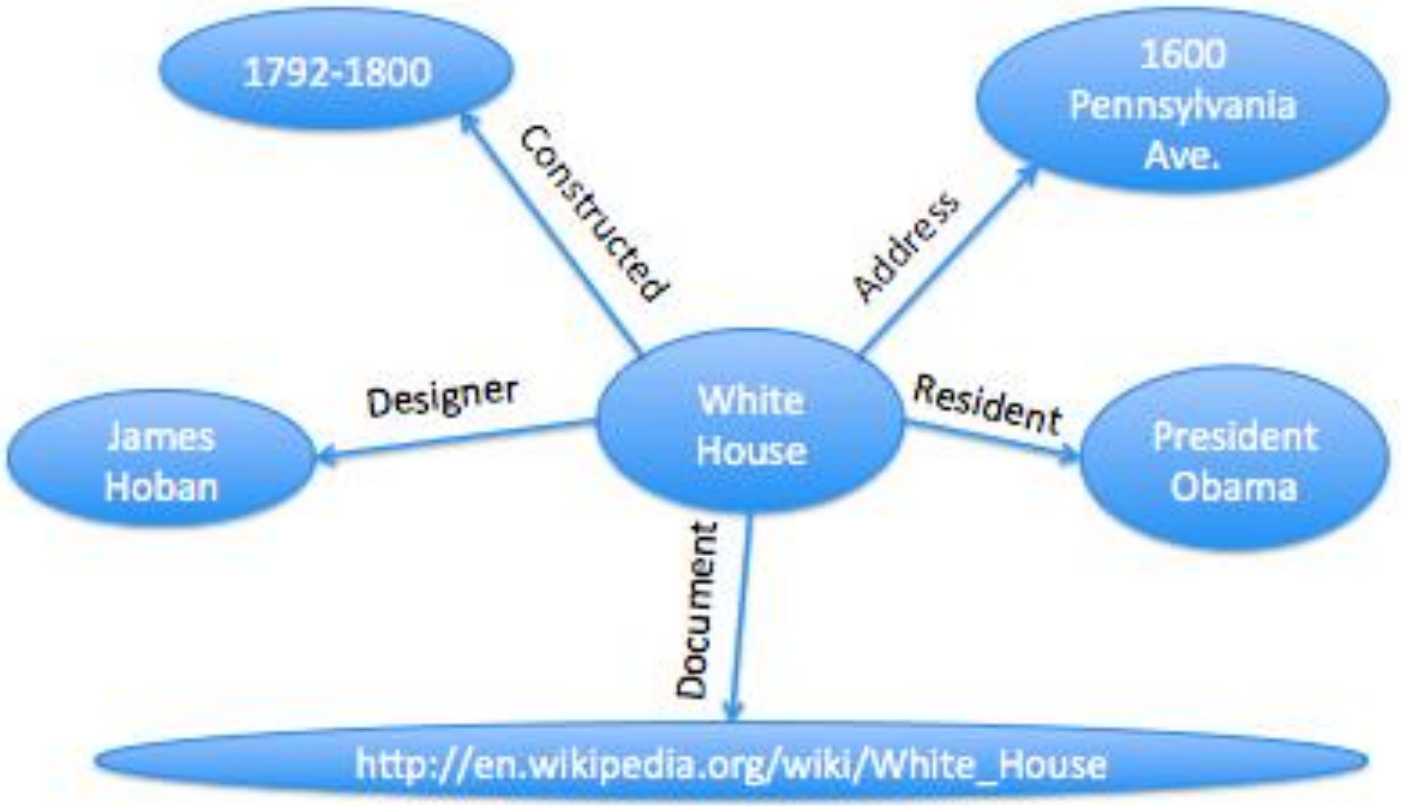
- Extension of the Web through **standards** by the World Wide Web Consortium (W3C). The standards promote common data formats and exchange protocols on the Web, most fundamentally the **Resource Description Framework (RDF).**



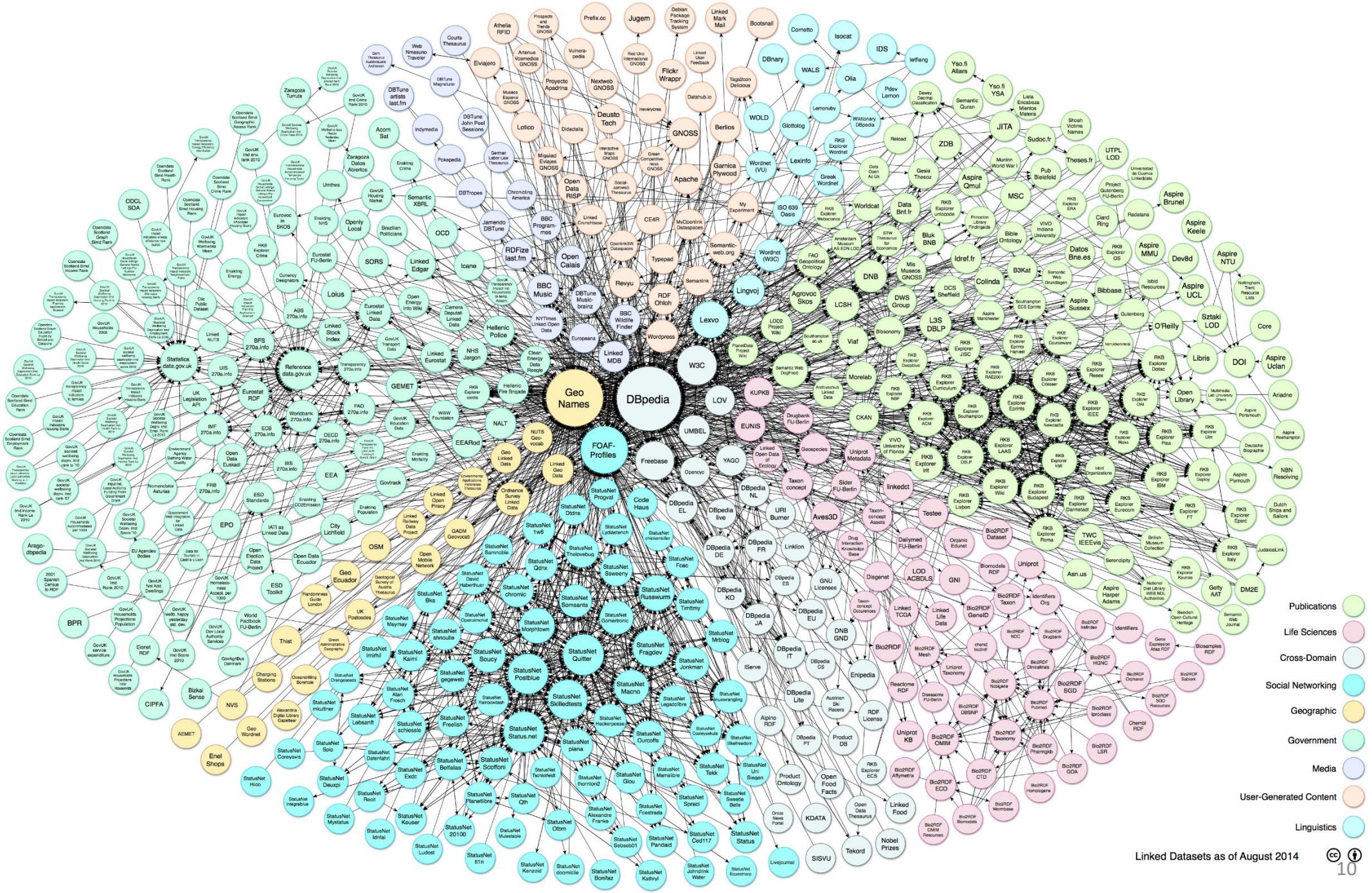
Background: Resource Description Framework (RDF)

- RDF is used as the standard way to describe and model information. Three object types conforms the basic model :
- **i) Resources.** The things that where RDF expressions are used to describe them.
- **ii) Properties.** The specific description of a resource, It can be an attribute or relation.
- **iii) Statements.** The conjunction of a resource, a named property and the value of that property. This 3 elements form the RDF statement of a specific resource. They are expressed in the form of subject, predicate, object and commonly called \triples". Triples create a basic **graph structure of data.**

From…

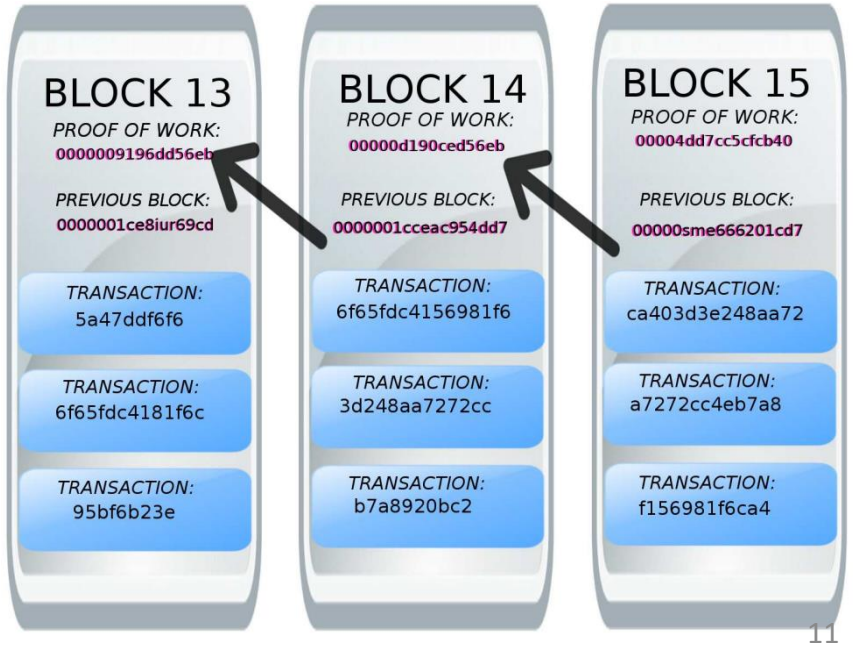

1792-1800
Constructed
1600 Pennsylvania Ave.
Address
James Hoban
Designer
White House
Resident
President Obama
Document
http://en.wikipedia.org/wiki/White_House


To...


Geo Names
DBpedia
FOAF-Profiles
Statistics data.gov.uk
Reference data.gov.uk
Publications
Life Sciences
Cross-Domain
Social Networking
Geographic
Government
Media
User-Generated Content
Linguistics
Linked Datasets as of August 2014

What is the **Blockchain?**

- Is a distributed database that maintains a continuously-growing list of records secured from tampering and revision. It consists of data structure blocks that may contain data or program with each block holding batches of individual transactions.

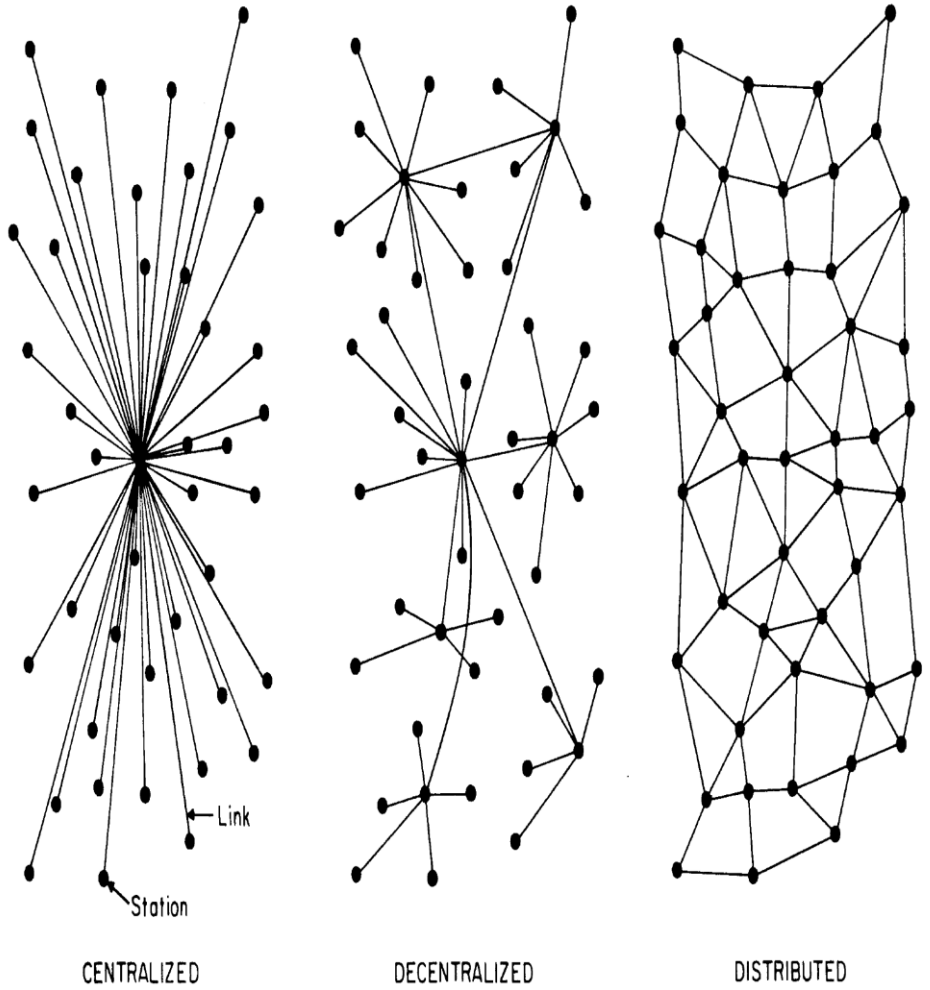


SOURCE: Matthew English, Sören Auer, and John Domingue. Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development, 2016.

Cryptocurrencies

Background: Bitcoin

- First decentralized digital cryptocurrency.
- First system using Blockchain.
- Borderless and instantaneous transactions.



Background: Ethereum

- General purpose cryptocurrency platform that offers a Turing complete virtual machine, based on Bitcoin technology.
- Possible to run any coin, script, or cryptocurrency project, as implementations of smart contracts.
- SMART CONTRACT: An algorithm that can self-execute, self-enforce, self-verify, and self-constrain the performance of a contract.

Background: Blockchain Benefits and Features

- Ownership of data.
- Uniqueness and proof of uniqueness.
- Immutability.
- Censorship resilient.
- Public transparency and traceability.
- Trustless and incorruptible.
- Cost-efficient.
- Guaranteed continuity.

Semantic Web benefits

- Consistency
- Standardization
- Linking and mappings

Semantic Web + Blockchain

+

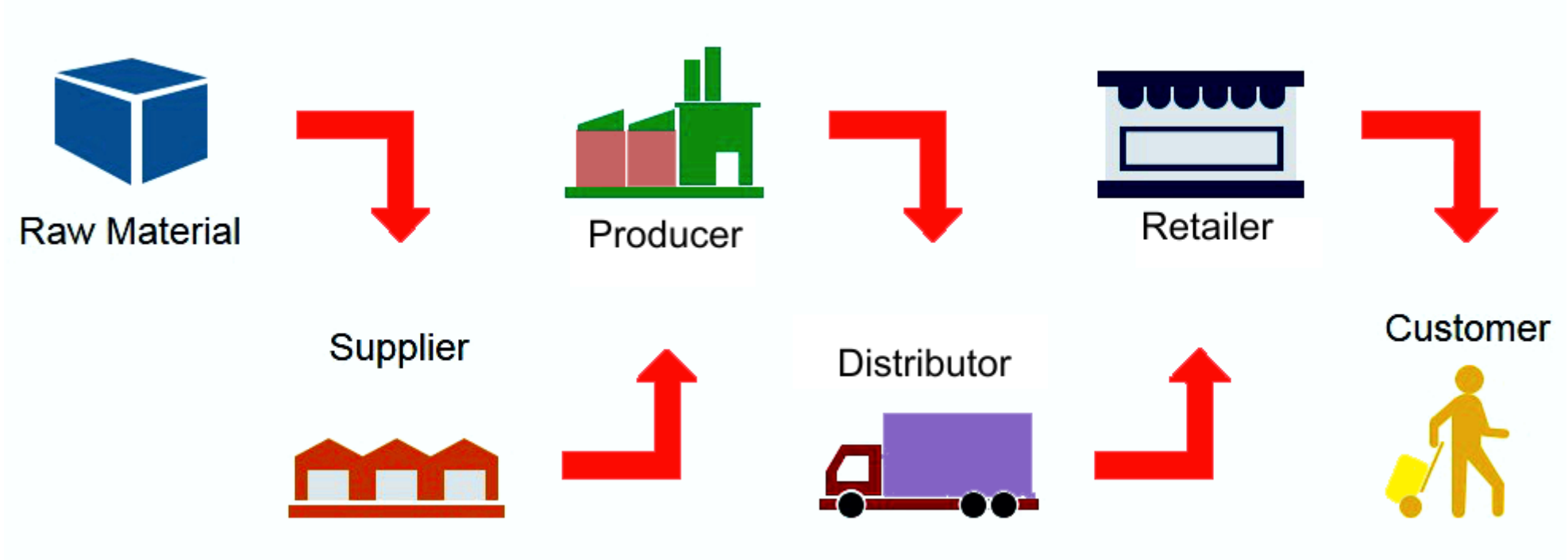
blockchain

Semantic Blockchain

Semantic Blockchain

- Semantic Blockchain is the use of Semantic web standards on blockchain based systems. The standards promote common data formats and exchange protocols on the blockchain, making used of the Resource Description Framework (RDF).

Background: Supply Chain

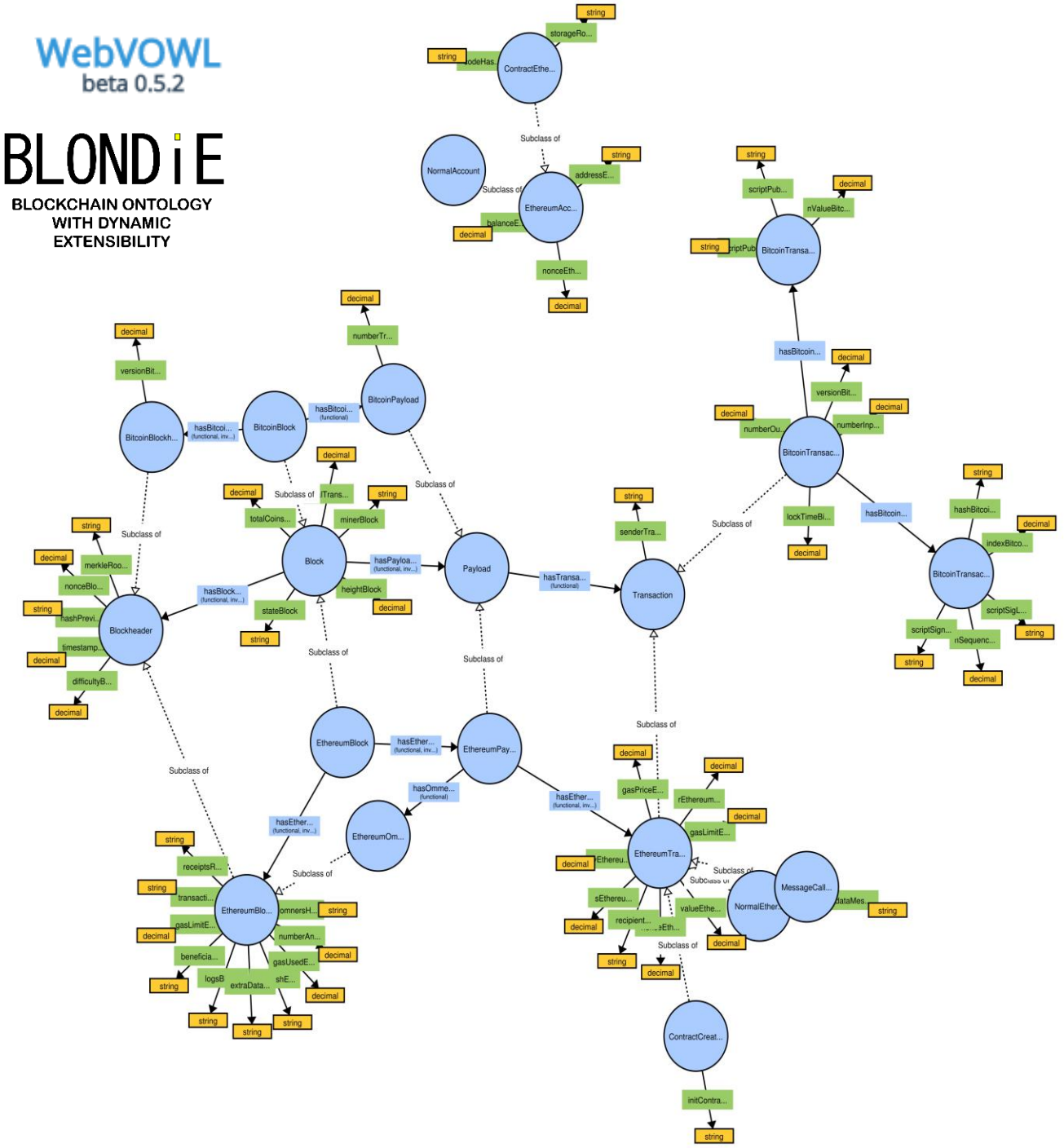


BLONDiE

WebVOWL
beta 0.5.2

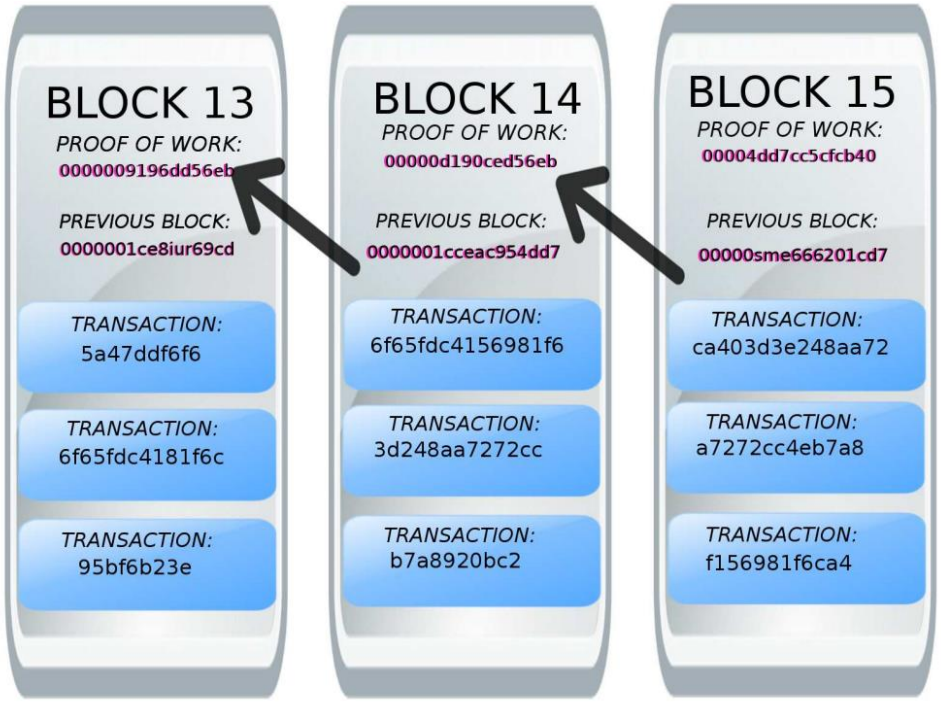
BLONDiE
BLOCKCHAIN ONTOLOGY
WITH DYNAMIC
EXTENSIBILITY

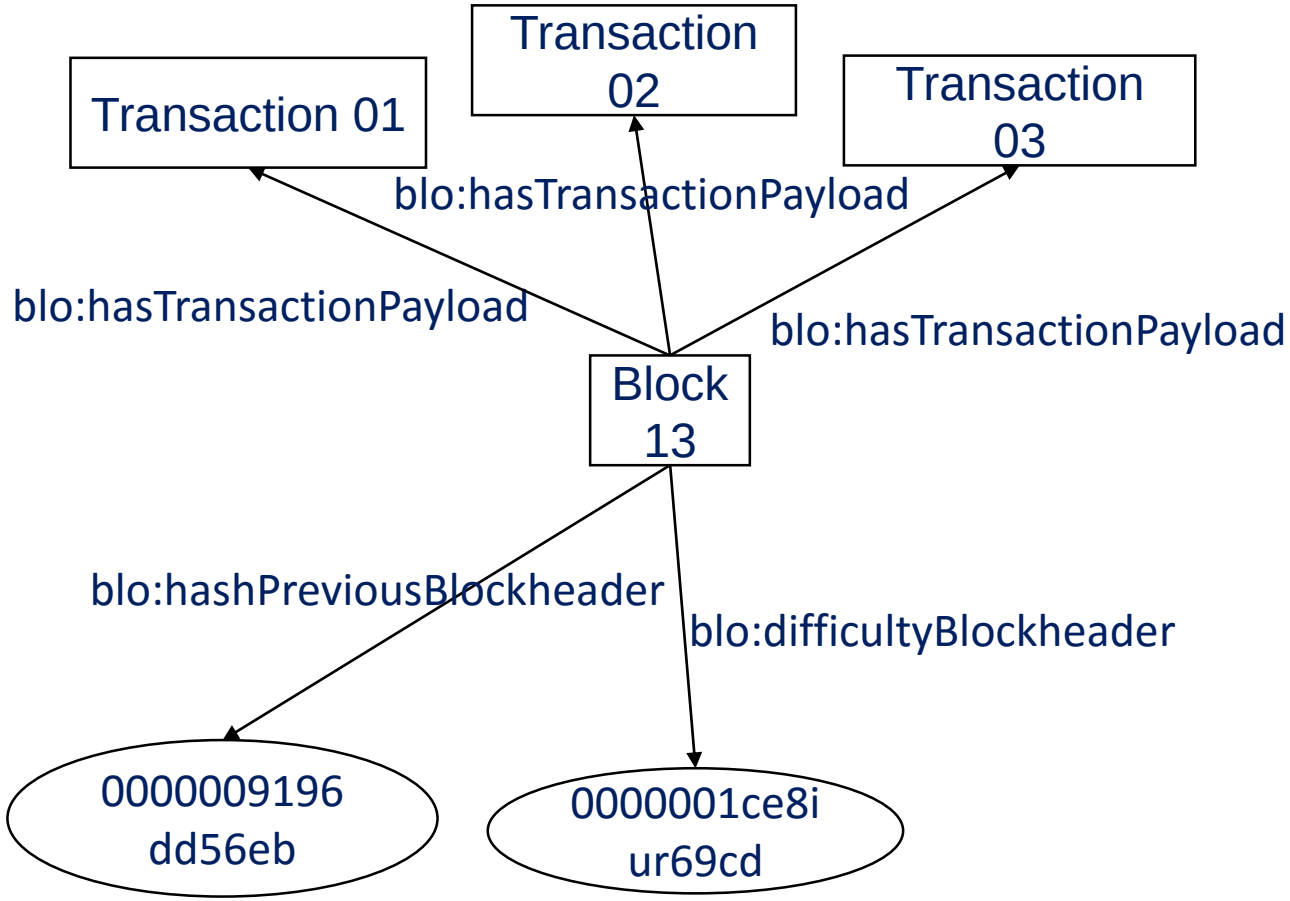
- Ethereum and Bitcoin.
- 21 classes.
- 11 object properties.
- 50 datatype properties.
- OWL Ontology: disjoint, domain, range, etc.
- Properties: functional, inverse functional, etc.



BLONDiE

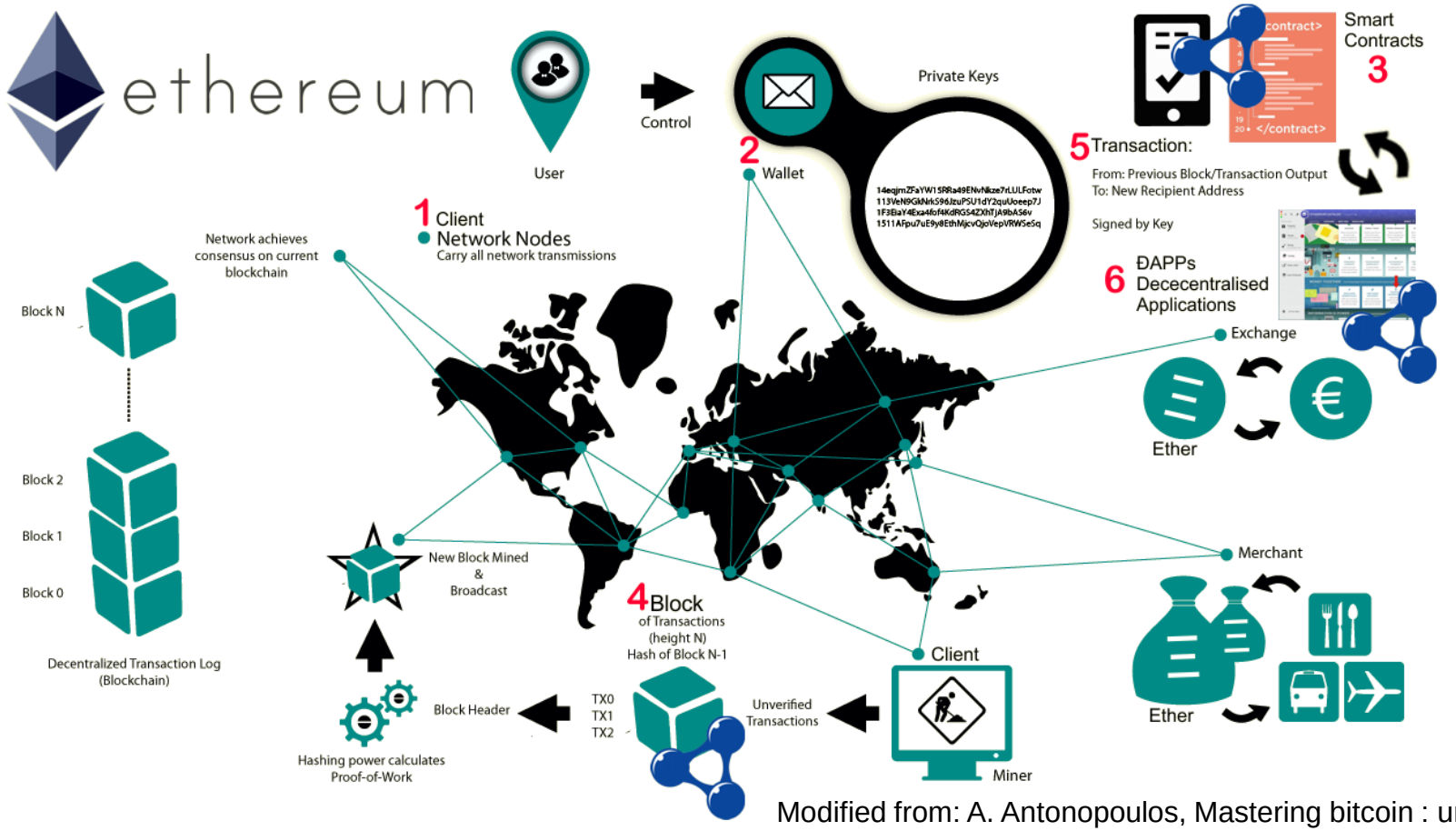
BLONDiE
BLOCKCHAIN ONTOLOGY WITH DYNAMIC EXTENSIBILITY





Matthew English, Sören Auer, and John Domingue. Block Chain Technologies & The Semantic Web: A Framework for Symbiotic Development, 2016.

Extracting Data and Storing RDF Data on Ethereum



Modified from: A. Antonopoulos, Mastering bitcoin : unlocking digital cryptocurrencies. Sebastopol, CA: O'Reilly, 2015.

RDF

ethereum

Extracting Data and Storing RDF Data on Ethereum

Task	Element	Way	Short Explanation	On Blockchain?
	1. Clients	JSON-RPC	Is a way to talk to an Ethereum node and receive as a response data related to different elements of the Ethereum framework.	No
Extracting data	2. Wallets	JSON files	Wallets are stored as JSON files facilitating the access to its data.	No
	3. Smart Contracts	ABI	The interface of the smart contract is shared in JSON format.	No
	4. Blocks	Extradata property	A data property to store at most 32 bytes.	Yes
Storing RDF Data	5. Transactions	Data property, Contract Storage, Event Logs, External Storage	Data can be stored in 4 possible ways on the transactions. Fees will be payed according to the size of the data. Each method offer different advantages and disadvantages.	Yes
	6. Đapps Interfaces	HTML Approaches	The interface of the Ethereum applications are usually done using HTML technologies. Therefore the usage of RDF data embedded on HTML is possible.	No

Extracting Data on Ethereum: Wallets

- {"address":"0xcb60081c79230499c5d5615505f88df53c5bbcc9",
"checksumAddress":"0xCB60081C79230499C5D5615505F88df53C5bBcC9","privKey":**"3c8f4ddb1cb78625dad5a221c28a873b37cc115f8ba243508eb338a908afeeb0"**,"pubKey":"0xdbb189772ec307e06242fefbdcb95bf0f21cc1ba0ba584d22db2f9a4e87d6f0fc231985dfb39dd6a54bb9f93e75428010e52e701ab05a09c9676419222ac2b7a","publisher":"MyEtherWallet","encrypted":false,"version":2}

Unencrypted wallet generated with myetherwallet.com

Storing RDF Data on Ethereum: Gas

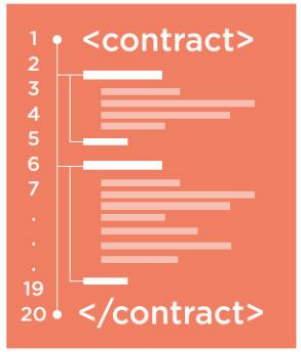
- Execution fee that a user has to pay on gas units for every operation made on the Ethereum Blockchain.
- Gas cost.
- Gas price.
- Gas limit.
- Gas fee.

Storing RDF Data on Ethereum: Transactions

-Way	Short explanation	Advantages	Disadvantages
Data property	Property existing in each transaction on Ethereum	- Not fixed size. - Cannot be modified	- Expensive - Stored on hexadecimal format - Is not SPV friendly
Contract Storage	Contract state flexible database. Key-value store	- Not fixed size - Easily Accesible	- Expensive - Information is modifiable
Event Logs	Historical raw data	- Cheap	- Not accesible for smart contracts. - Data generated by the smart contract
External Storage (IPFS)	Storing it externally and keeping the identi er using one of the above methods	Unlimited size	- Not guaranteed that data will not be removed

Storing RDF Data on Ethereum: Contract Storage & IPFS

```
contract Sample {
  string rdfData = "RDF Data Here ";
}
```



key-value store with 2^{256} possible keys and 2^{256} values

IPFS

```
contract Sample {
  string rdfData = “IPFS Hash Here ";
}
```

e.g. QmYwAPJzv5CZsnA625s3Xf2nemtYgPpHdWEz79ojWnPbdG

The current problem

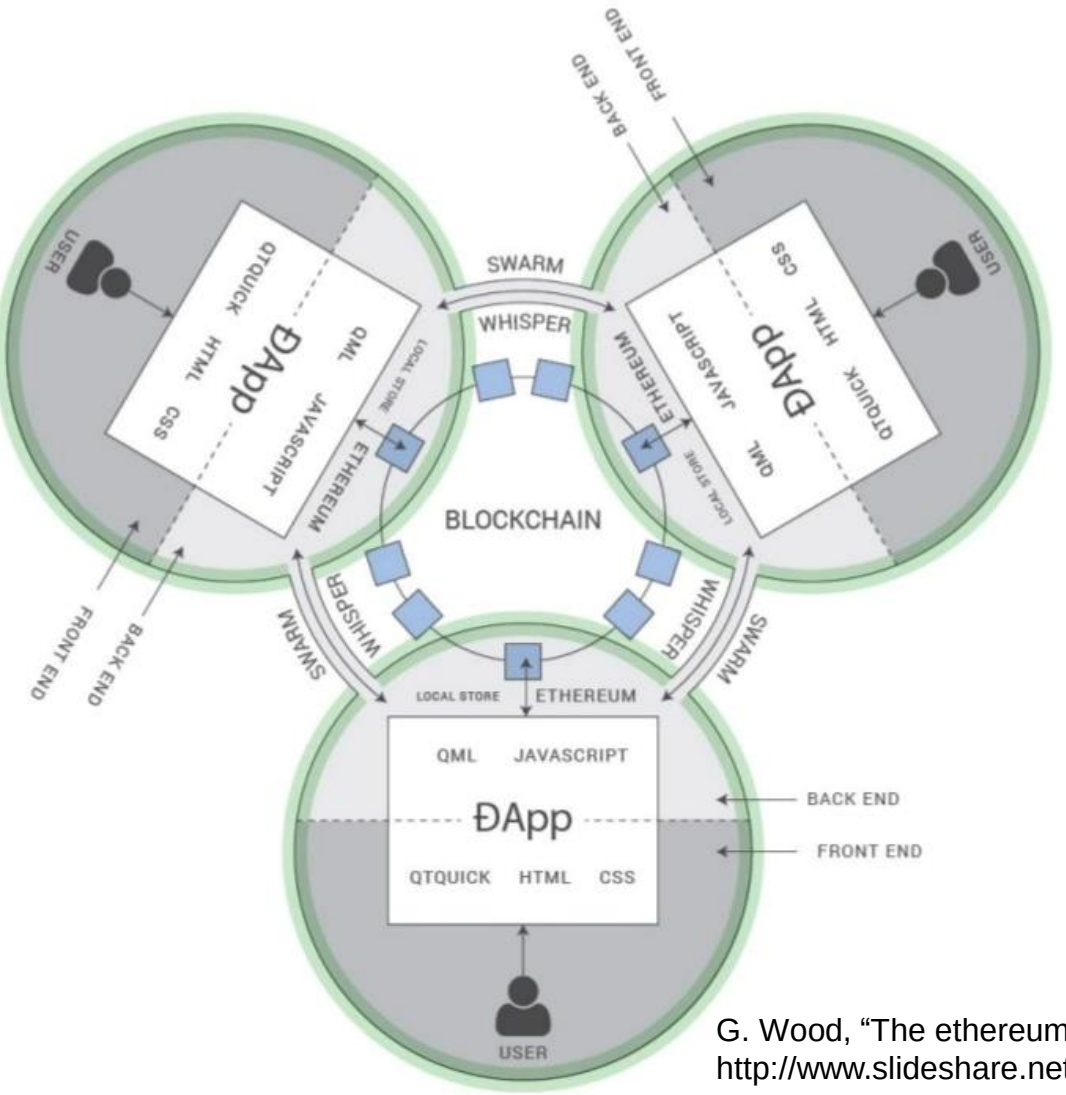
- Existing Suppy Chain systems are heterogeneous.
- It is expensive and they are not reliable.
- Tracking and tracing is not easy.
- EXAMPLE: **2013 Horse meat scandal!**

DeSCA prototype

- Ethereum Decentralized Application.
- Basic Supply Chain Management prototype.
- Record flow of goods.
- Record data participants.
- Record RDF data.

DeSCA

Architecture

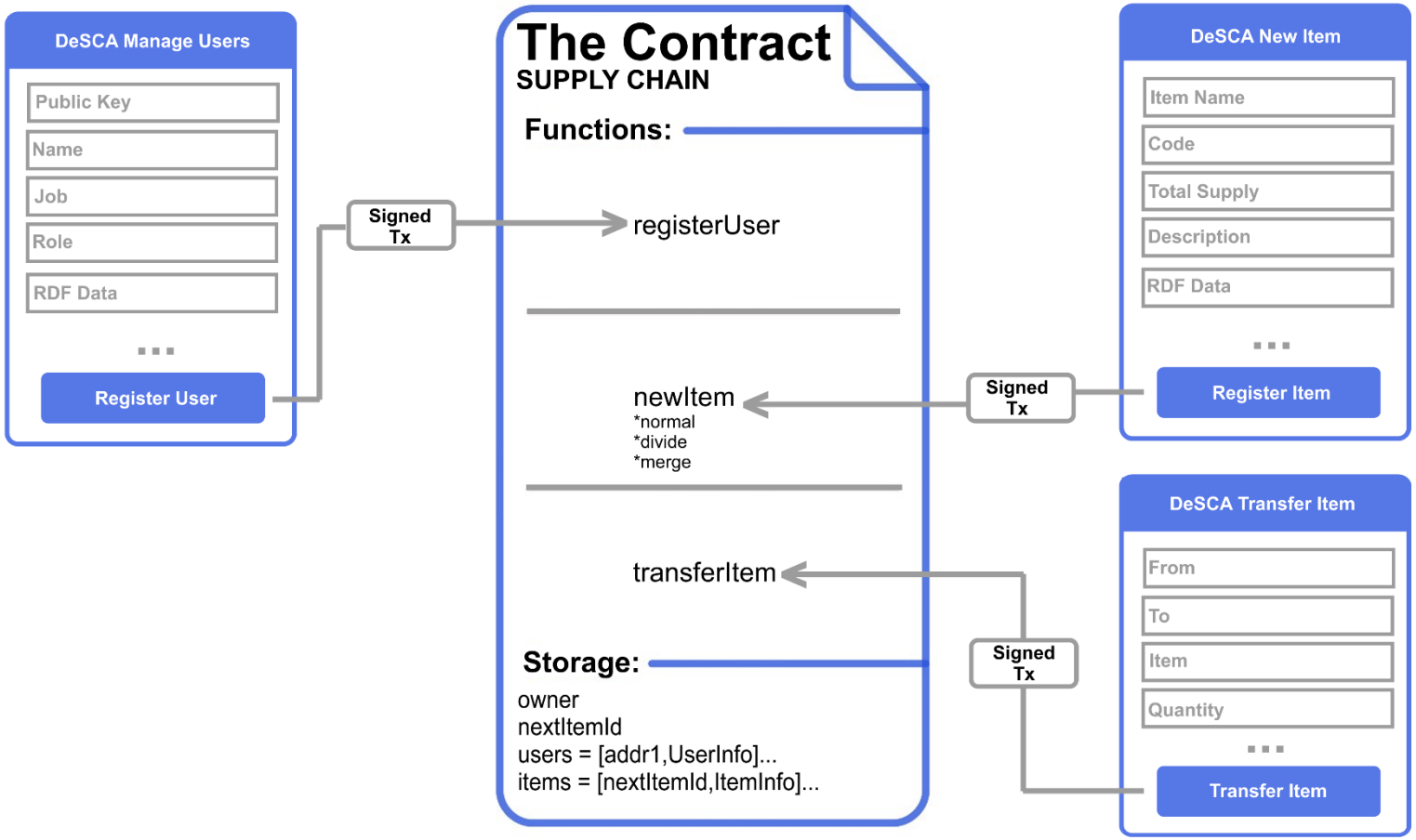


G. Wood, “The ethereum experience." [Online]. Available: http://www.slideshare.net/ethereum/the-ethereum-experience

Functionalities

- Create account
- Manage smart contract
- Register user
- Create item
- Transfer item
- Show provenance

DeSCA: Smart Contract



```
contract SupplyChain {
  address public owner;
  uint public nextItemId = 0;

  struct User{
    string name;
    string jobTitle;
    string company;
    string role;
    string rdfData;
  }

  struct Item{
    string name;
    string code;
  //  uint8 decimals;
    uint256 totalSupply;
    string description;
    string rdfData;
    mapping (address => uint256) balanceOf;
  }

  mapping (address => User) public users;
  mapping (uint256 => Item) public items;


event Test(uint _nextItemId);
event Transfer(address _from, address _to, uint _id, uint256 _value);
event Register(address _userAddress, string _name, string _role);
//event Register(address _userAddress);
event Creation(uint _nextItemId, string _name, uint256 _totalsupply, address _ownerItem, string _type);
//event Creation(uint _nextItemId, uint256 _totalsupply, address _ownerItem);
event NewItemNormal(uint _nextItemId, string _name, string _code, uint256 _totalSupply, string _description);
event NewItemDivide(uint _nextItemId, string _name, string _code, uint256 _totalSupply, string _description, uint _id, uint256 _quantity);
event NewItemMerge(uint _nextItemId, string _name, string _code, uint256 _totalSupply, string _description, uint _id1 , uint _id2, uint256 _quantity1, uint256 _quantity2);
```

Programming languages and frameworks

web3.js

ipfs.js

Evaluation

Meetup

Bitcoin Cologne

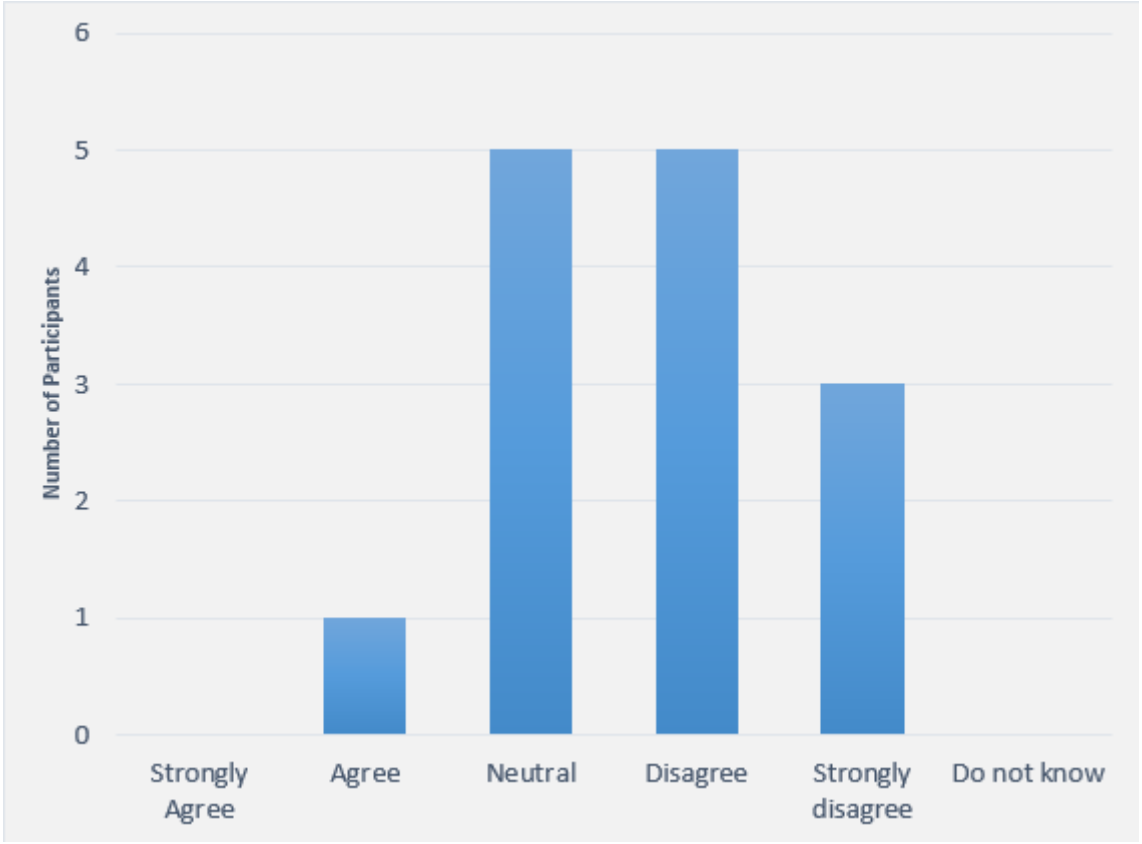
Evaluation

- 14 participants different profiles.
- Most of them informed about Blockchain technologies.
- Technology awareness.
- Usability evaluation.

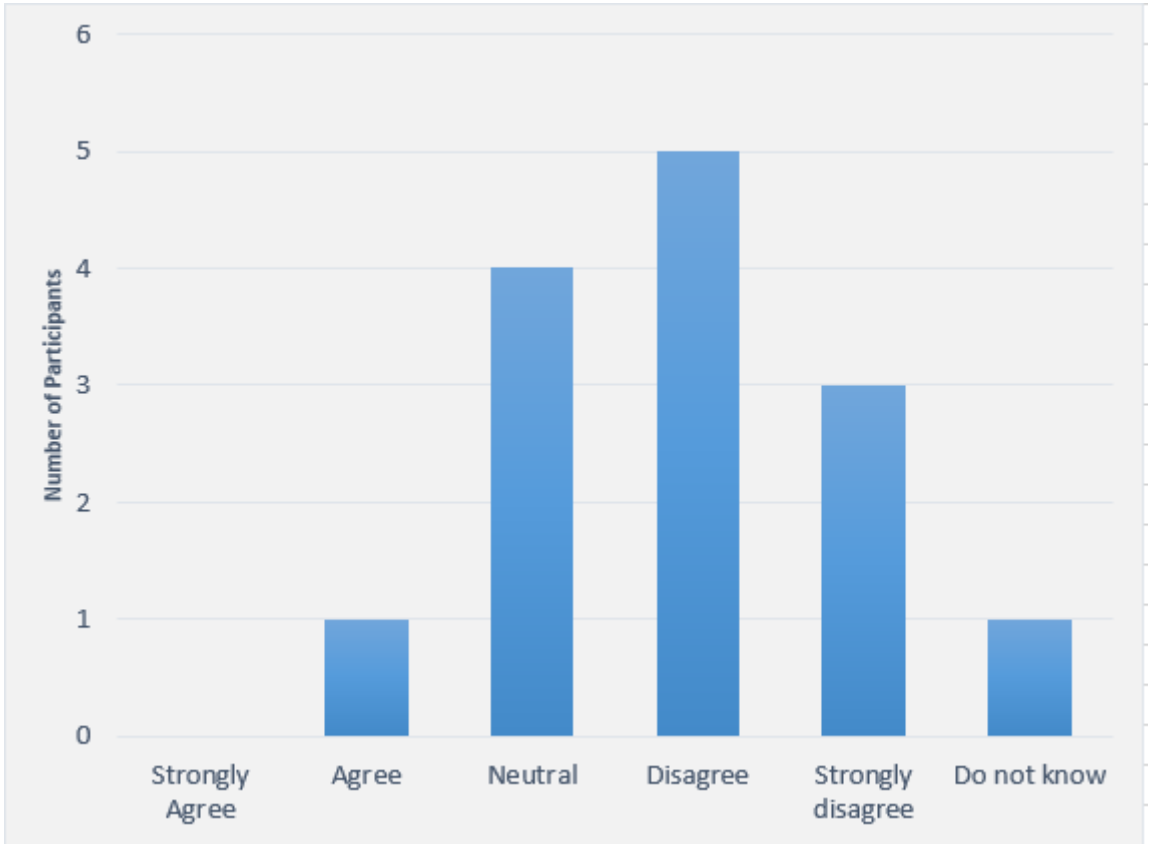
Evaluation: Technology awareness

- Around **93%** participants knew before about Blockchain.
- Around **85%** participants knew before about Semantic web.
- **100%** of participants think that Semantic Web is useful.
- Around **85%** participants knew before about SCM.

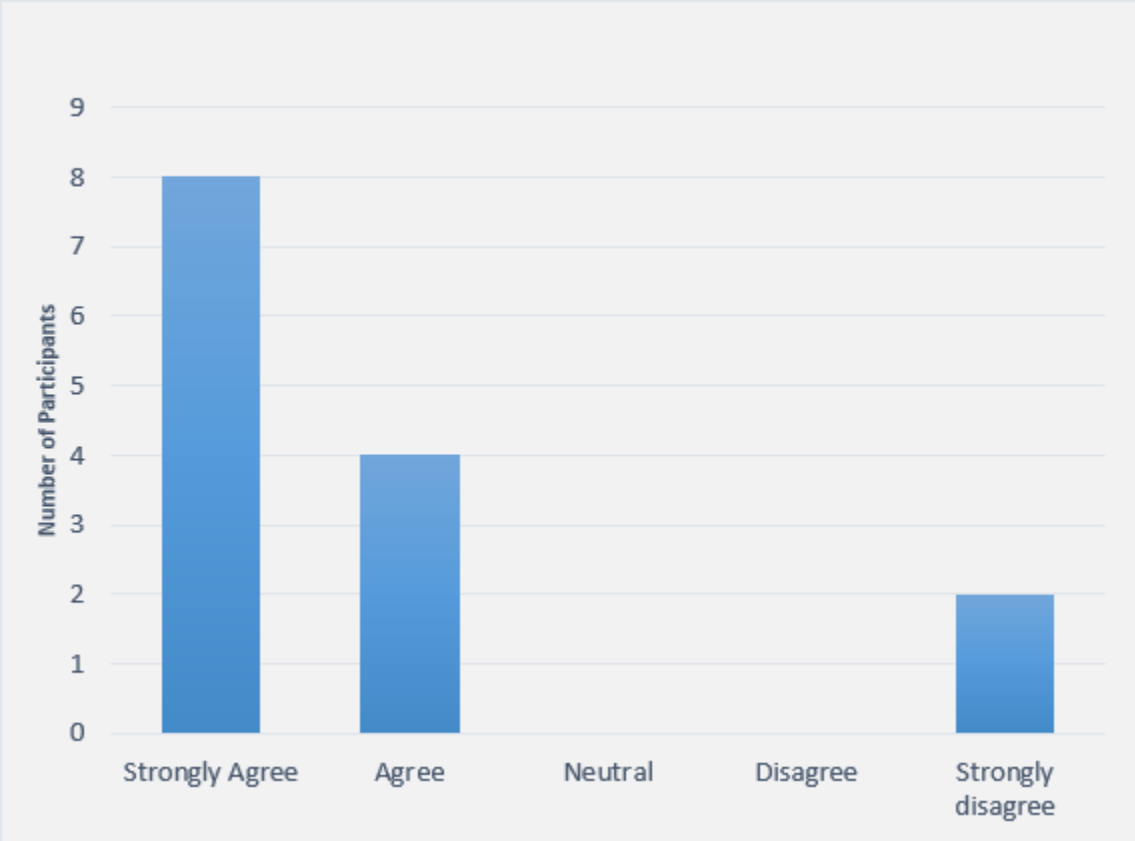
Evaluation: “The prototype is not easy to understand”



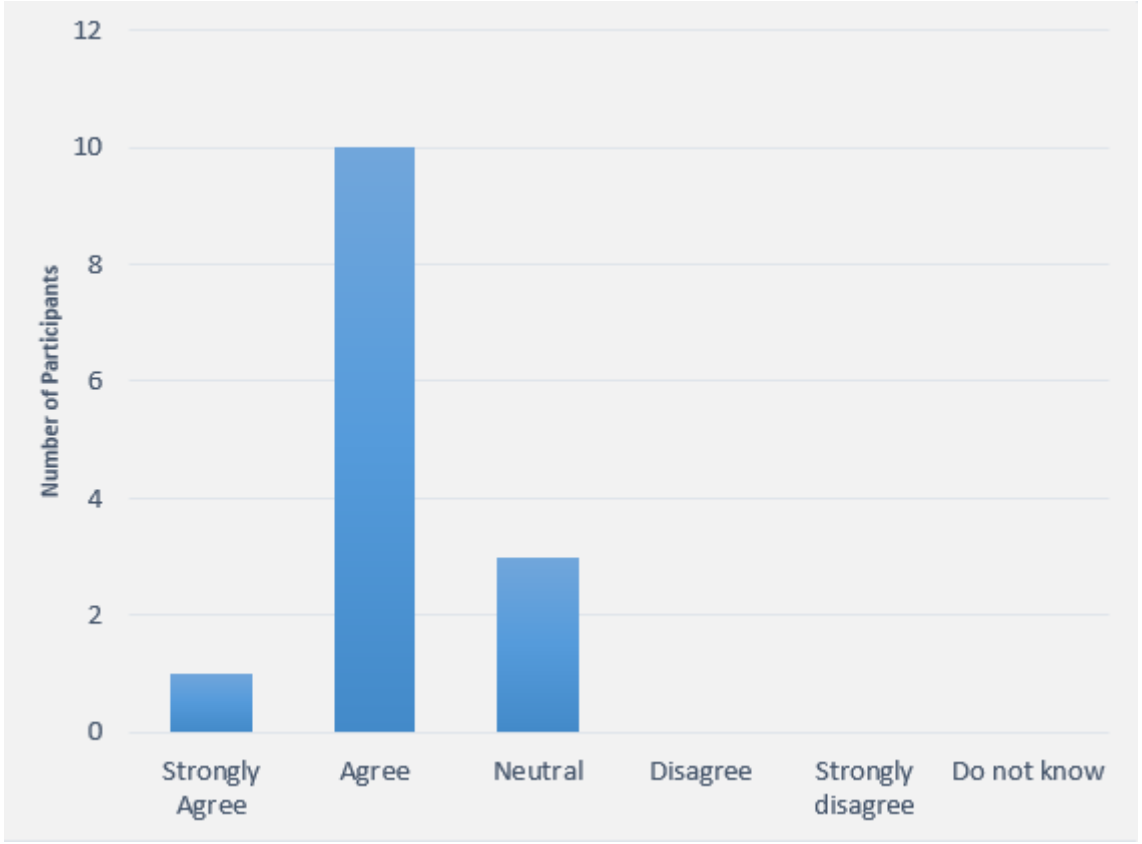
Evaluation: “It is not a useful prototype for Supply Chain Management”



Evaluation: “It is easy to learn”



Evaluation: “The prototype has benefits compared to possible centralized solutions”



Conclusions

- This research presented some integrations steps between Semantic and Blockchain technologies.
- BLONDiE: OWL ontology.
- Extracting data and storing RDF data from Ethereum.
- DeSCA: Ethereum ĐApp prototype for SCM.
- DeSCA was evaluated resulting that most people think it is easy to understand, is useful, easy to learn, and offers advantages compared to centralized systems.

Future Work

- BLONDiE can be extended to cover more Blockchain-based platforms (Hyperledger, NXT, etc).
- Research about more Semantic integration on Ethereum like instead of using HTTP-URIs, start using hashes as identifiers.
- DeSCA can be extended to cover more data related to SCM. It can be extended to allow manage of users and item data, store certificates that prove origin of data.

Descriptive Scenario

Name	Job Title	Company	Role
Eric Cartman	Farmer	Daisy Hill Puppy Farm	Producer
Ellie Williams	CEO	Umbrella Corp.	Distributor
Apu Nahasapeemapetilon	Owner	Kwik-E-Mart	Retailer
Milhouse Van Houten	Student	University of Bonn	Customer

DeSCA

https://youtu.be/JiWDYByK5zo

Thanks