

# Semantic Blockchain

Mentor: *Prof. Dr. Maria-Esther Vidal*

Team Members: *Firas, Ernane, Matthew*



Craig Wright will publish “extraordinary proof” that he is Satoshi

TechCrunch - 13 hours ago

Another day, another confirmation that the shadowy figure called Satoshi Nakamoto is ...

Craig Wright Says He Will Prove He Is Bitcoin Creator 'Satoshi Nakamoto'

Wall Street Journal - 11 hours ago

The Bitcoin affair: Craig Wright promises extraordinary proof

BBC News - 19 hours ago

[More news for craig wright](#)

---

Craig Wright's signature is worthless : Bitcoin - Reddit

[https://www.reddit.com/r/Bitcoin/.../craig\\_wrights\\_signature\\_is\\_worthless...](https://www.reddit.com/r/Bitcoin/.../craig_wrights_signature_is_worthless...) ▼

2 days ago - JoukeH [discovered]

([https://www.reddit.com/r/Bitcoin/comments/4hf4xj/creator\\_of\\_bitcoin\\_reveals\\_identity/d2pf70v](https://www.reddit.com/r/Bitcoin/comments/4hf4xj/creator_of_bitcoin_reveals_identity/d2pf70v))  
that the signature on **Craig**.

# Notable Addresses

## 1A1zP1eP5QGefi2DMPTfTL5SLmv7DivfNa

**The Genesis Address** – the very first bitcoin address. It's assumed to be controlled by Satoshi Nakamoto, although the btc has never moved. There is a technical issue that prevents the original 50 BTC from being transacted.

Total Received: 65.44021956 BTC

Current Balance: 65.44021956 BTC

Notable transactions: 50 BTC, the genesis of bitcoin, and then a steady stream of smaller amounts, some with public notes of gratitude to Satoshi.

## 1Ez69SnzzmePmZX3WpEzMKTrcBF2gpNQ55

**US Marshals** – the destination of the bitcoins nabbed from Ross Ulbricht and the Silk Road investigation, then auctioned off. Before the auctions of this and other U.S. Marshal controlled bitcoins, the federal government was considered to be the largest holders of bitcoin, aside from the addresses controlled by Satoshi Nakamoto. This fact ruffled the feathers of not a few libertarian minded bitcoiners.

Total Received: 29,658.80913195 BTC

Current Balance: 0.01073195 BTC

Notable transactions: 29,658 BTC to Tim Draper [1a8LDh3qtCdMFAgRXzMrdrvB8w1EG4h1Xi](#), as well as what appear to be novelty tips.

# Transaction Analysis

## Bitcoin Address

[Home](#) / Address: 12c6DSiU4Rq3P4ZxziKxzl5LmMBrzjrjX

Hash	12c6DSiU4Rq3P4ZxziKxzl5LmMBrzjrjX
------	-----------------------------------

Balance	50.02869420 BTC
---------	-----------------

Total received	50.02869420 BTC
----------------	-----------------

Transactions	36
--------------	----

Unconfirmed	0.00000000 BTC
-------------	----------------

*Note: Unconfirmed balance is not part of the address balance or total.*



# Transaction Analysis

Main info

Transactions

Transaction tree

First Transaction

Time

2009-01-09 03:54:25

Block

1

Transaction

0e3e2357e806b6cdb1f70b54c3a3a17b6714ee1..

Amount

50.00000000 BTC

Confirmations

409273

Last Transaction

Time

2016-04-04 14:08:38

Block

405700

Transaction

0c95ae7a1be95740a5892465376efa322bc798f...

Amount

0.00060941 BTC

Confirmations

3574

# Relational Database Model

→ Bitcoin Block Explorer (BBE)

→ Blockchain.info

public.addr
id: serial
hash160: text
type: integer
addr_pkey
addr_hash160_index
addr_hash160_type_index

public.blk
id: serial
hash: bytea
depth: integer
version: bigint
prev_hash: bytea
mrkl_root: bytea
time: bigint
bits: bigint
nonce: bigint
blk_size: integer
chain: integer
work: bytea
date: date
blk_pkey
blk_depth_index
blk_hash_index
blk_hash_key
blk_id_index
blk_prev_hash_index
blk_time_index

public.addr_txout
addr_id: integer
txout_id: integer
addr_txout_addr_id_index
addr_txout_txout_id_index

public.blk_tx
blk_id: integer
tx_id: integer
idx: integer
blk_tx_blk_id_index
blk_tx_tx_id_index

public.txout
addr_id: integer
txout_id: integer
tx_id: integer
tx_idx: integer
pk_script: bytea
value: bigint
type: integer
date: date
txout_addr_id_index
txout_date_index
txout_pk_script_index
txout_tx_id_index
txout_tx_idx_index
txout_txout_id_index
txout_type_index
txout_value_index

public.tx
id: integer
hash: bytea
version: bigint
lock_time: bigint
coinbase: boolean
tx_size: integer
nhash: bytea
maxout: integer
maxin: integer
tx_id_index
tx_maxin_index
tx_maxout_index

public.txin
id: serial
tx_id: integer
tx_idx: integer
prev_out_index: bigint
sequence: bigint
script_sig: bytea
prev_out: bytea
p2sh_type: integer
txin_pkey
txin_id_p2sh_type_index
txin_prev_out_prev_out_index_in...
txin_tx_id_index

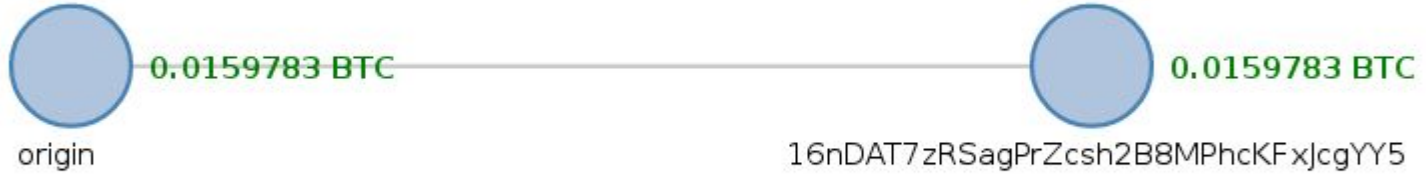
# Transaction Analysis

→ Triplestore Data Model

Inputs	Address balance	Outputs
<b>0.00060941</b> 2016-04-04 14:08:38	50.02869420	
<b>0.00092000</b> 2016-04-04 13:41:04	50.02808479	
<b>0.00005470</b> 2016-02-01 13:56:54	50.02716479	
<b>0.00005470</b> 2016-02-01 13:39:56	50.02711009	
<b>0.00005470</b> 2016-02-01 13:39:56	50.02705539	
<b>0.00010000</b> 2016-01-06 04:10:55	50.02700069	

# Status Quo

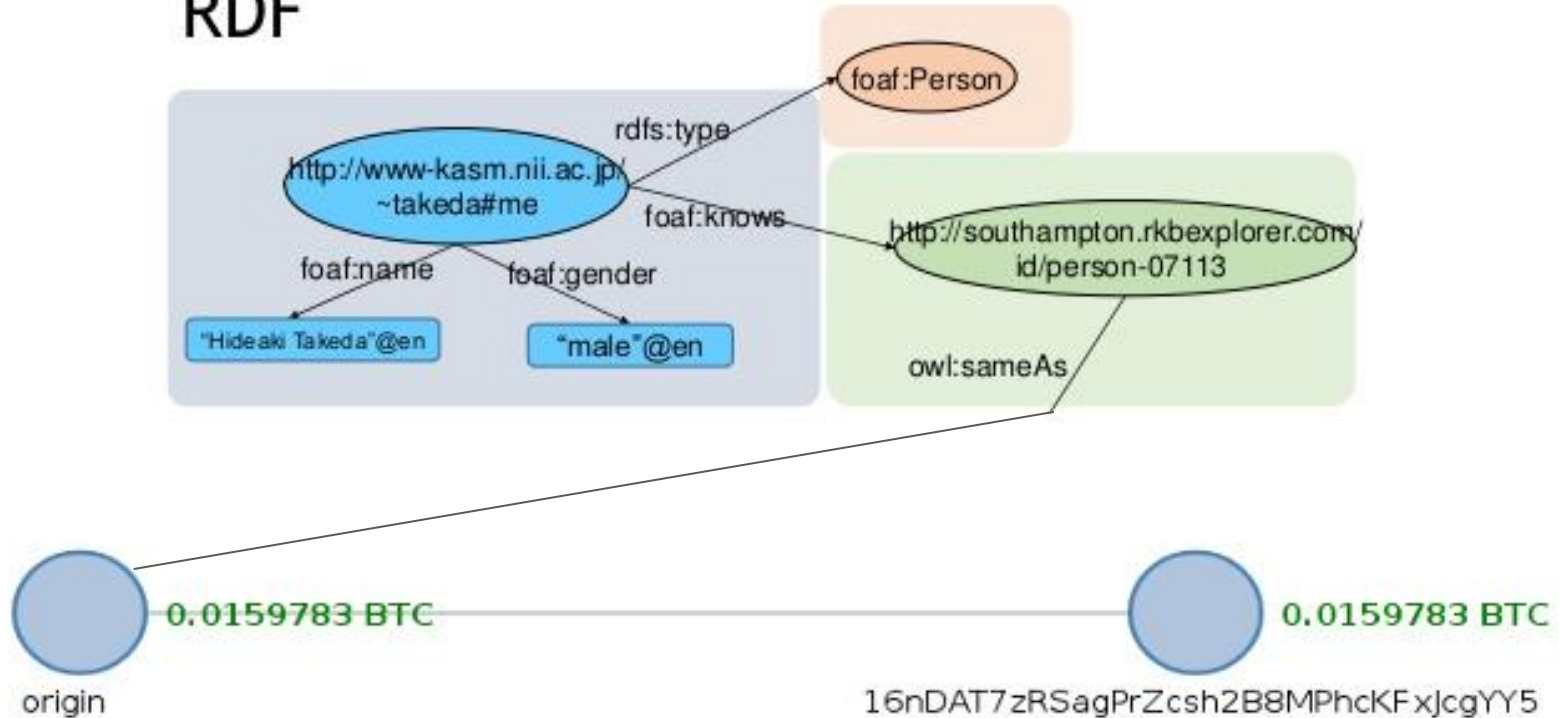
⋮  
|



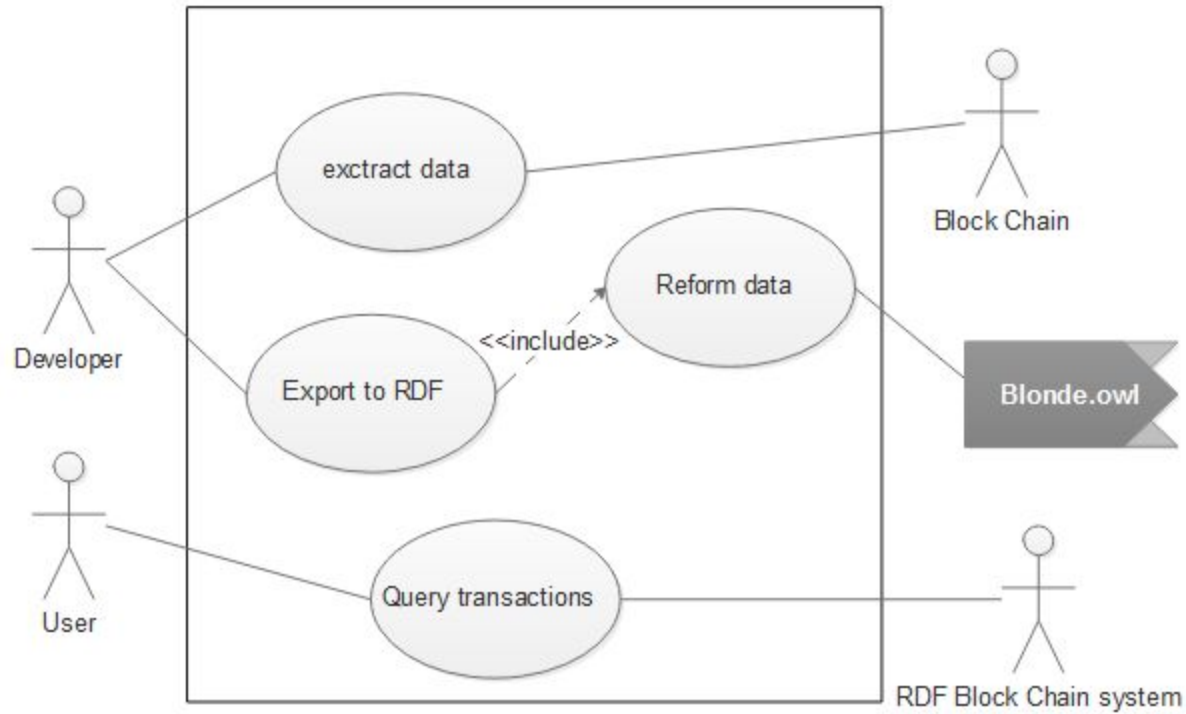


# Data Enhancement

## RDF



# Use Case



# User Interface

## Home Welcome to Blockchain

[More...](#)

Height	Age	Transactions	Total Sent	Relayed By	Size (kB)
<a href="#">410168</a>	5 minutes	2545	24,772.91 BTC	<a href="#">BitFury</a>	998.08
<a href="#">410167</a>	22 minutes	2090	17,225.59 BTC	<a href="#">AntPool</a>	998.05
<a href="#">410166</a>	32 minutes	3098	32,947.95 BTC	<a href="#">AntPool</a>	998.17
<a href="#">410165</a>	56 minutes	2024	22,037.33 BTC	<a href="#">AntPool</a>	998.07
<a href="#">410164</a>	1 hour 6 minutes	2691	34,444.14 BTC	<a href="#">AntPool</a>	998.11
<a href="#">410163</a>	1 hour 28 minutes	2351	20,429.93 BTC	<a href="#">BitFury</a>	998.19

### Latest Transactions

<a href="#">b82a41ae50c51ee8e405c50cf...</a>	< 1 minute	0.07534672 BTC
<a href="#">2d01b63383beb033df92d8d2d...</a>	< 1 minute	0.01348473 BTC
<a href="#">b30a77e77d5145f5a10509f74...</a>	< 1 minute	3.8337595 BTC
<a href="#">4a927d338a338ad84a4a9b70f...</a>	< 1 minute	2.40 BTC
<a href="#">882d2149e6dc3a68d84cf4a5c...</a>	< 1 minute	0.49459964 BTC
<a href="#">88d8c5221d9554bd4d6da28c5...</a>	< 1 minute	12.96774727 BTC
<a href="#">02599d8e577d0f78051ec69a0...</a>	< 1 minute	72.39101795 BTC

### Search

You may enter a block height, address, block hash, transaction hash, hash160, or ipv4 address...

### NEWS

Magnr - Bitcoin Trading Platform | Trade with Leverage

Magnr ← 1 minute ago

€500, the 'Bin Laden' of banknotes, could be axed

/r/bitcoin 6 minutes ago

Gavin breaks Twitter silence: "In my head today: Truth is stranger than fiction. And: People are weird."

/r/btc 27 minutes ago

# ***Applications and Future Aspects***

- Data mining (graph mining) to identify patterns.
- More efficient queries.
- Link to Open Data Cloud.
- Facilitate Blockchain 2.0 applications.
- Android Application (Semantic Wallet)
- ...

