Analysis of Bitcoin Transaction Flows to Reveal Usage and Geographic Patterns

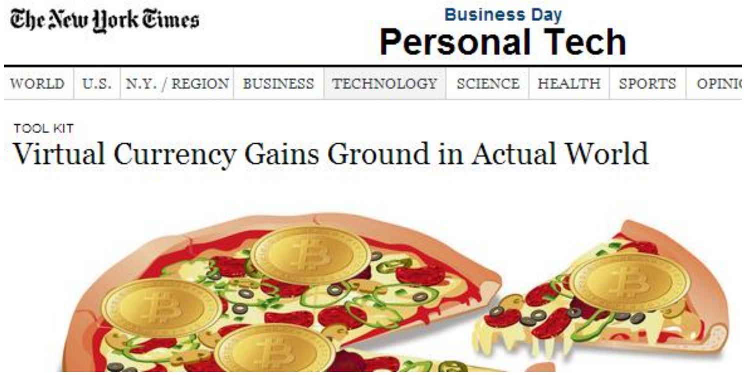
Shiva P. Bissessar

Supervisor: Dr. Nicolas T. Courtois

University College London
M.Sc. Information Security

Thesis
2013

Bitcoin’s Wave of Popularity



The New York Times

Business Day

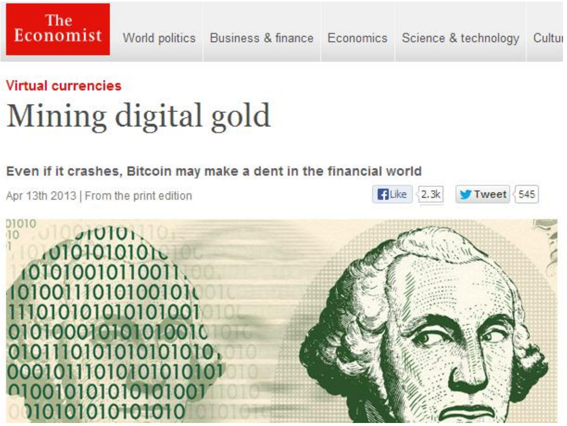
Personal Tech

WORLD U.S. N.Y. / REGION BUSINESS TECHNOLOGY SCIENCE HEALTH SPORTS OPINI

TOOL KIT

Virtual Currency Gains Ground in Actual World

- The New York Times, 1st August 2013



The Economist

World politics Business & finance Economics Science & technology Cultu

Virtual currencies

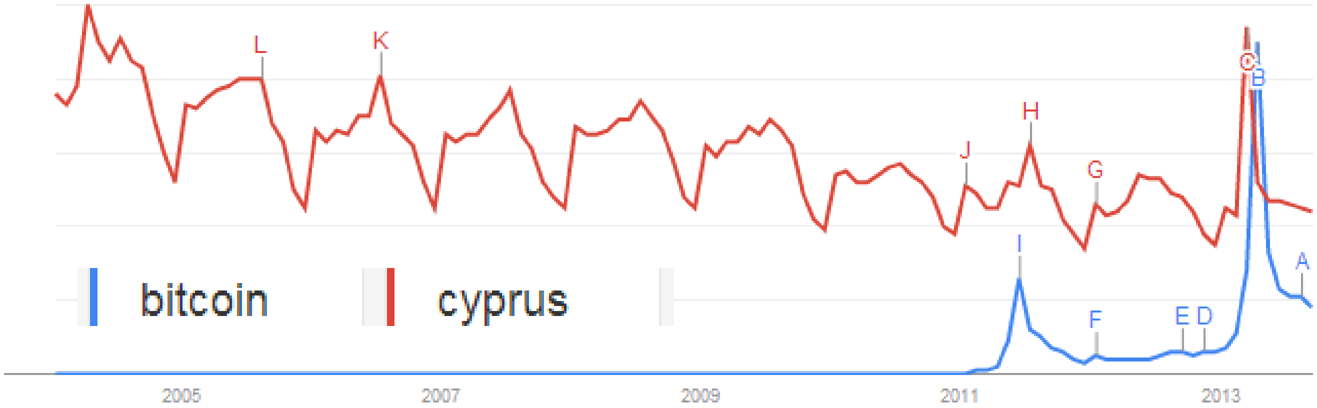
Mining digital gold

Even if it crashes, Bitcoin may make a dent in the financial world

Apr 13th 2013 | From the print edition

Like 2.3k Tweet 545

- The Economist, 13th April 2013



- Google Trends showing spike in usage and high correlation between terms “Bitcoin” and “Cyprus” around March/April 2013

Technical, Analytical & Regulatory Timeline

2008, 2009, 2010

Nov 2008:

Satoshi Nakamoto publishes paper

Jan 2009:

Genesis Block created

Jul 2010:

Mt. Gox Bitcoin exchange established

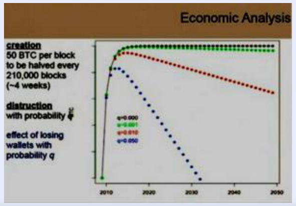
2011

Jul:

Academic paper by Reid and Harrigan shows Bitcoin is not anonymous

Dec:

28C3 conference where Hamacher and Katzenbeisser paradoxically predicts Bictoin supply falls to zero over time



2012

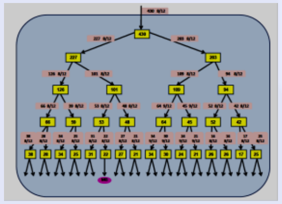
Apr:

FBI paper on Bitcoin's potential facilitating illicit activities

Oct:

ECB report classifies Bitcion as virtual currency

Ron and Shamir paper show 78% supply of Bitcoin dormant and tracing results



Nov:

Miners' reward (coinbase) halved to 25BTC

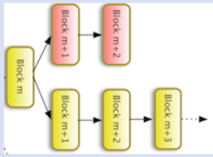
WordPress begins accepting Bitcoin

2013

Mar:

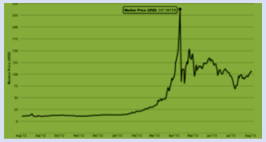
US: FinCEN guidelines encompassing aspects of Bitcoin ecosystem within their remit

Software incompatibility results in Blockchian fork



Apr:

BTC value exceeds $250 USD in wake of Cyprus instability

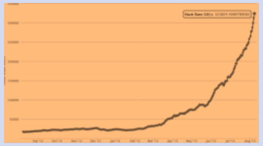


May:

Dan Kaminsky announces CPU/GPU friendly proof of works changes inevitable due to ASIC domination

Aug 2013

ASIC miners push hash rate beyond 300 Terra-Hash



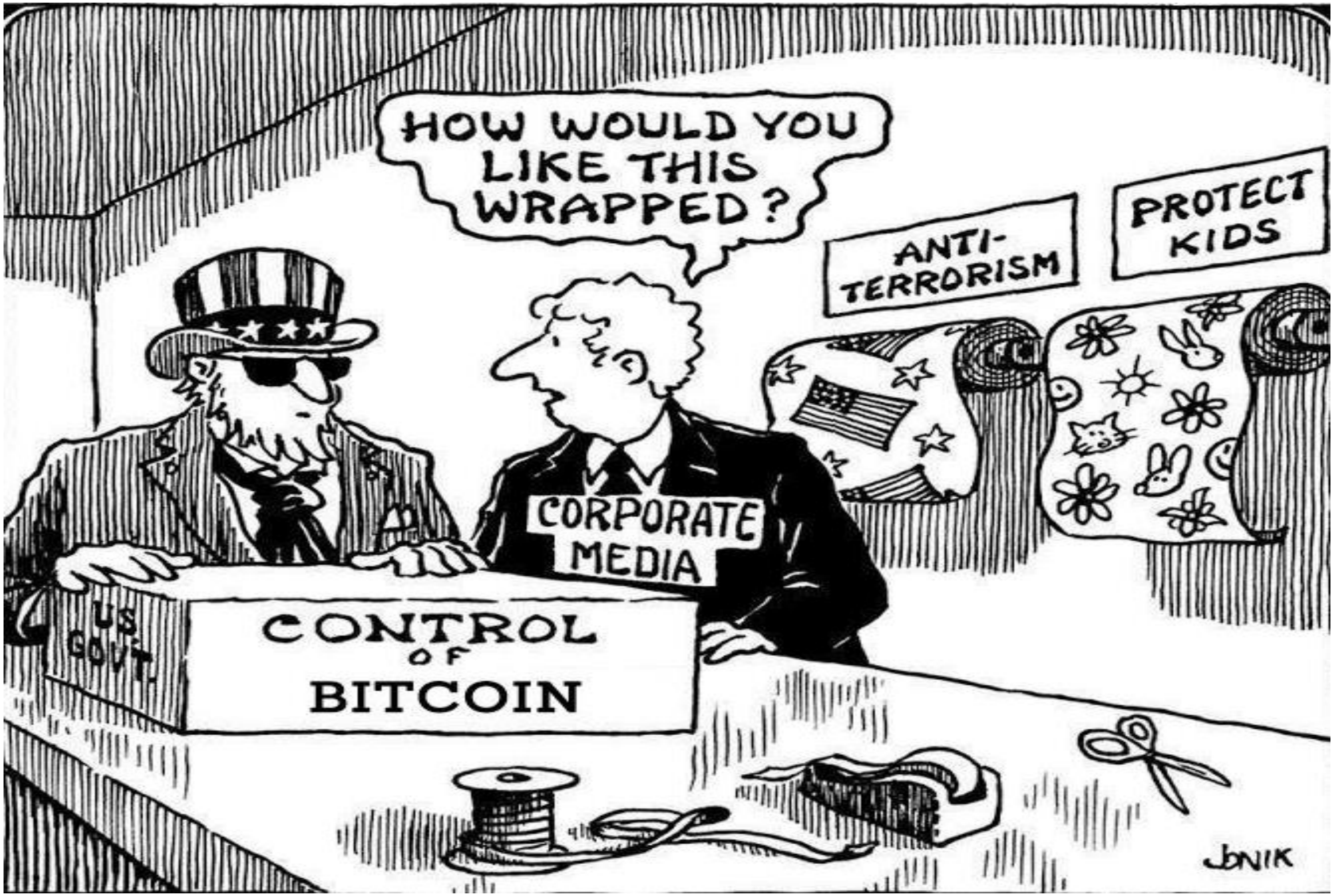
US legal precedent; "Bitcoin is a currency or form of money"

Germany announces Bitcoin is "Private Money"

Thailand companies trading Bitcoin cease operations as central bank reviews Bitcoin

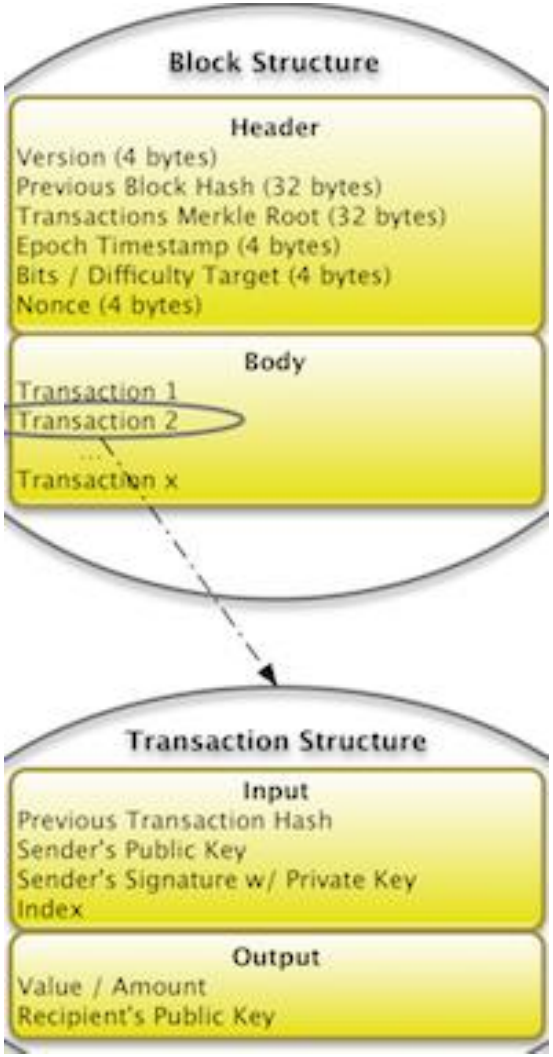
State of NY subpoenas for information

Increasing Regulatory Attention Translates To Need For Understanding Usage And Geographic Patterns



http://i.imgur.com/TAHgUPy.jpg

Examining The Blockchain And Constituent Transactions



http://www.javaworld.com/javaworld/jw-11-2011/Images/bitcoin2_fig1.png

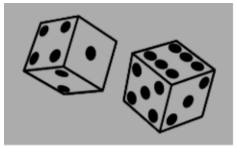
Two Python programs created to parse large volumes of transactions from the Blockchain as hosted by online communities resources

1. Parse 250K randomly collected transactions as a representative sample of all Bitcoin transactions for IP address information

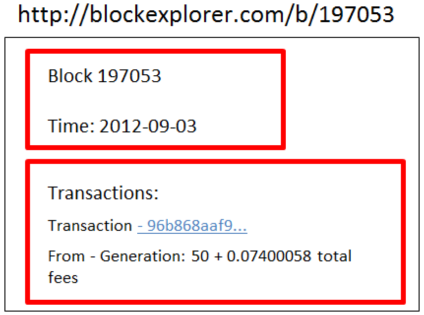
2. Collect a representative sample of transactions tracing coinbase ‘rewards’ from block generation all the way through to a dormant state

   - 70K transactions focusing on summarized block level results
   - 60K transactions with additional focus on IP address information

Random Traversal Of Blockchain To Acquire Representative Sample Of Transactions



1) Weighted random choice favouring selection of blocks with higher coinbase or 'reward' value



http://blockexplorer.com/b/197053

Block 197053

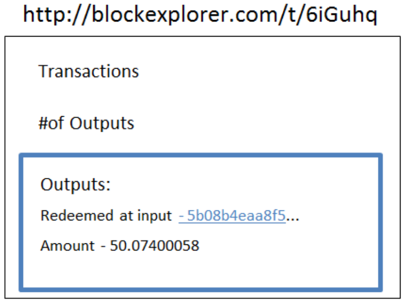
Time: 2012-09-03

Transactions:

Transaction - 96b868aaf9...

From - Generation: 50 + 0.07400058 total fees

2) Get block details on http://blockexplorer.com



http://blockexplorer.com/t/6iGuhq

Transactions

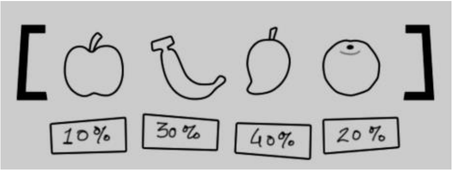
#of Outputs

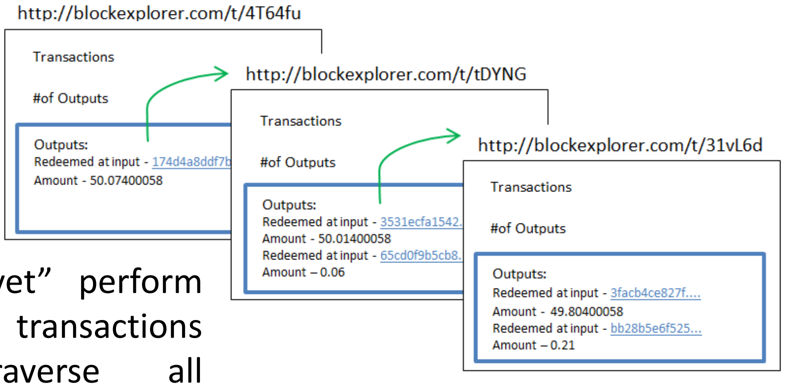
Outputs:

Redeemed at input - 5b08b4eaa8f5...

Amount - 50.07400058

3) Get details from block's coinbase transaction





http://blockexplorer.com/t/4T64fu

Transactions

#of Outputs

Outputs:
Redeemed at input - 174d4a8ddf7b
Amount - 50.07400058

http://blockexplorer.com/t/tDYNG

Transactions

#of Outputs

Outputs:
Redeemed at input - 3531ecfa1542.
Amount - 50.01400058
Redeemed at input - 65cd0f9b5cb8.
Amount – 0.06

http://blockexplorer.com/t/31vL6d

Transactions

#of Outputs

Outputs:
Redeemed at input - 3facb4ce827f....
Amount - 49.80400058
Redeemed at input - bb28b5e6f525...
Amount – 0.21

4) While "Not redeemed yet" perform weighted choice on output transactions amounts and randomly traverse all transactions recording transaction details

Blockchain

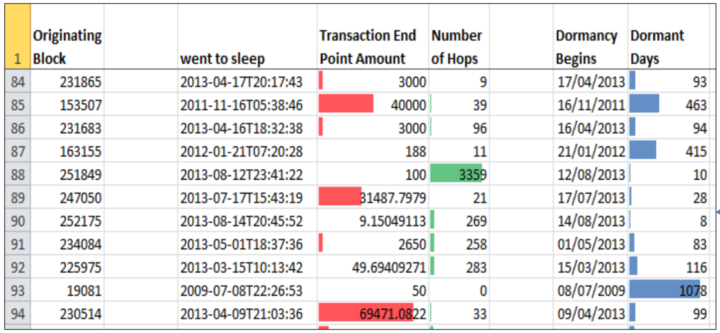
Block #197053

5) Get IP address data from http://blockchain.info and convert to country

6) Output transaction files

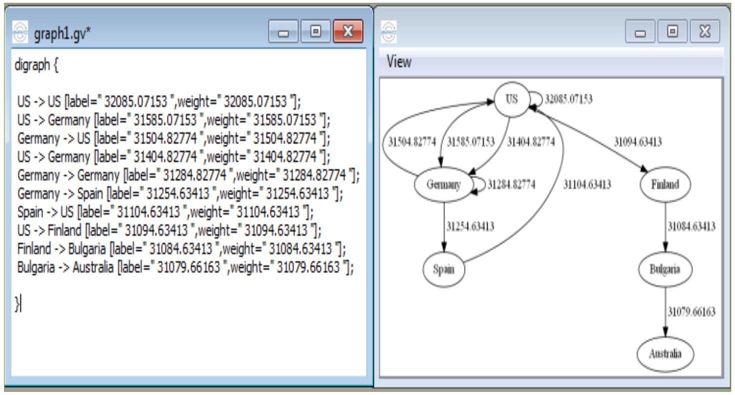
Data Analysis & Visualization

- Visualize and identify transactions for closer inspection:
  - High number of hops
  - High dormant amount
  - High dormant days.



1	Originating Block		went to sleep	Transaction End Point Amount	Number of Hops		Dormancy Begins	Dormant Days
84	231865		2013-04-17T20:17:43	3000	9		17/04/2013	93
85	153507		2011-11-16T05:38:46	40000	39		16/11/2011	463
86	231683		2013-04-16T18:32:38	3000	96		16/04/2013	94
87	163155		2012-01-21T07:20:28	188	11		21/01/2012	415
88	251849		2013-08-12T23:41:22	100	3359		12/08/2013	10
89	247050		2013-07-17T15:43:19	31487.7979	21		17/07/2013	28
90	252175		2013-08-14T20:45:52	9.15049113	269		14/08/2013	8
91	234084		2013-05-01T18:37:36	2650	258		01/05/2013	83
92	225975		2013-03-15T10:13:42	49.69409271	283		15/03/2013	116
93	19081		2009-07-08T22:26:53	50	0		08/07/2009	1078
94	230514		2013-04-09T21:03:36	69471.0822	33		09/04/2013	99

.xlsx

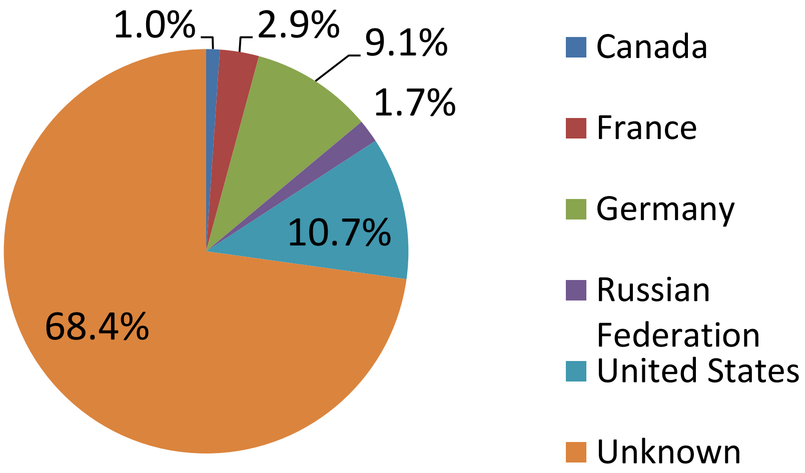


```
digraph {

 US -> US [label=" 32085.07153 ",weight=" 32085.07153 "];
 US -> Germany [label=" 31585.07153 ",weight=" 31585.07153 "];
 Germany -> US [label=" 31504.82774 ",weight=" 31504.82774 "];
 US -> Germany [label=" 31404.82774 ",weight=" 31404.82774 "];
 Germany -> Germany [label=" 31284.82774 ",weight=" 31284.82774 "];
 Germany -> Spain [label=" 31254.63413 ",weight=" 31254.63413 "];
 Spain -> US [label=" 31104.63413 ",weight=" 31104.63413 "];
 US -> Finland [label=" 31094.63413 ",weight=" 31094.63413 "];
 Finland -> Bulgaria [label=" 31084.63413 ",weight=" 31084.63413 "];
 Bulgaria -> Australia [label=" 31079.66163 ",weight=" 31079.66163 "];

}
```

- Digraphs were created using open source tool Graphviz to visualize selected transaction flows

- Dormancy period = period from date “Not yet redeemed” to 27th August 2013
- Only Dormancy periods greater than 90 days considered.

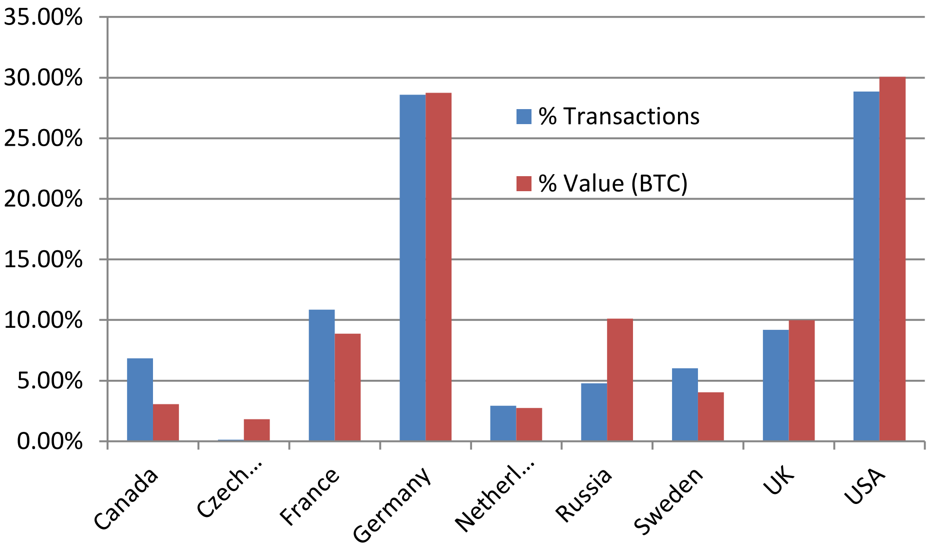
IP Address/Country Data Analysis



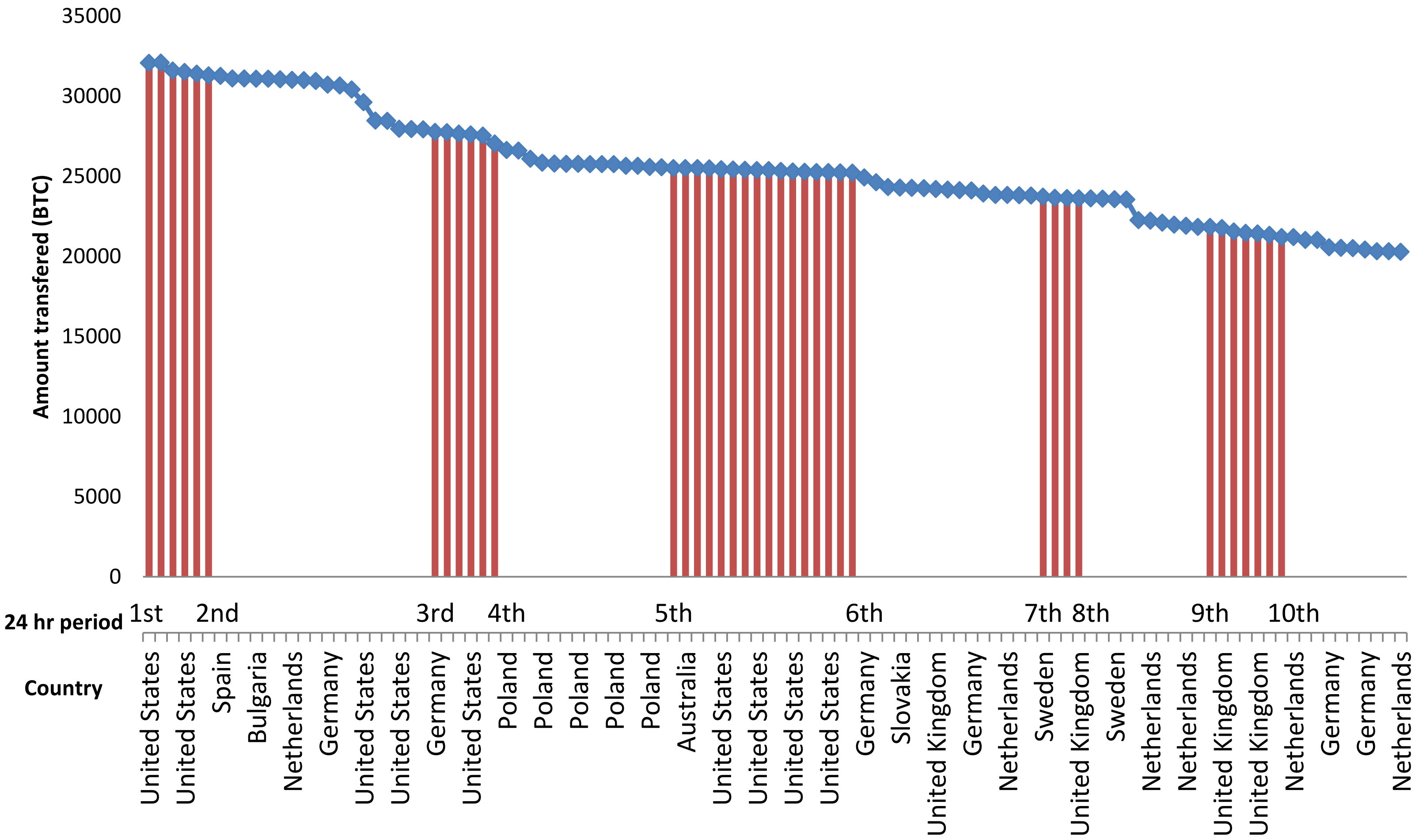
- 68% of the value within the total transaction sum of was attributable to “Unknown”. This implies high value transactions may be occurring using tools like “Tor” to annoymize identities

- Canada has higher percentage of transactions than Russia, however, Russia has almost 3 times as much transactional value than Canada

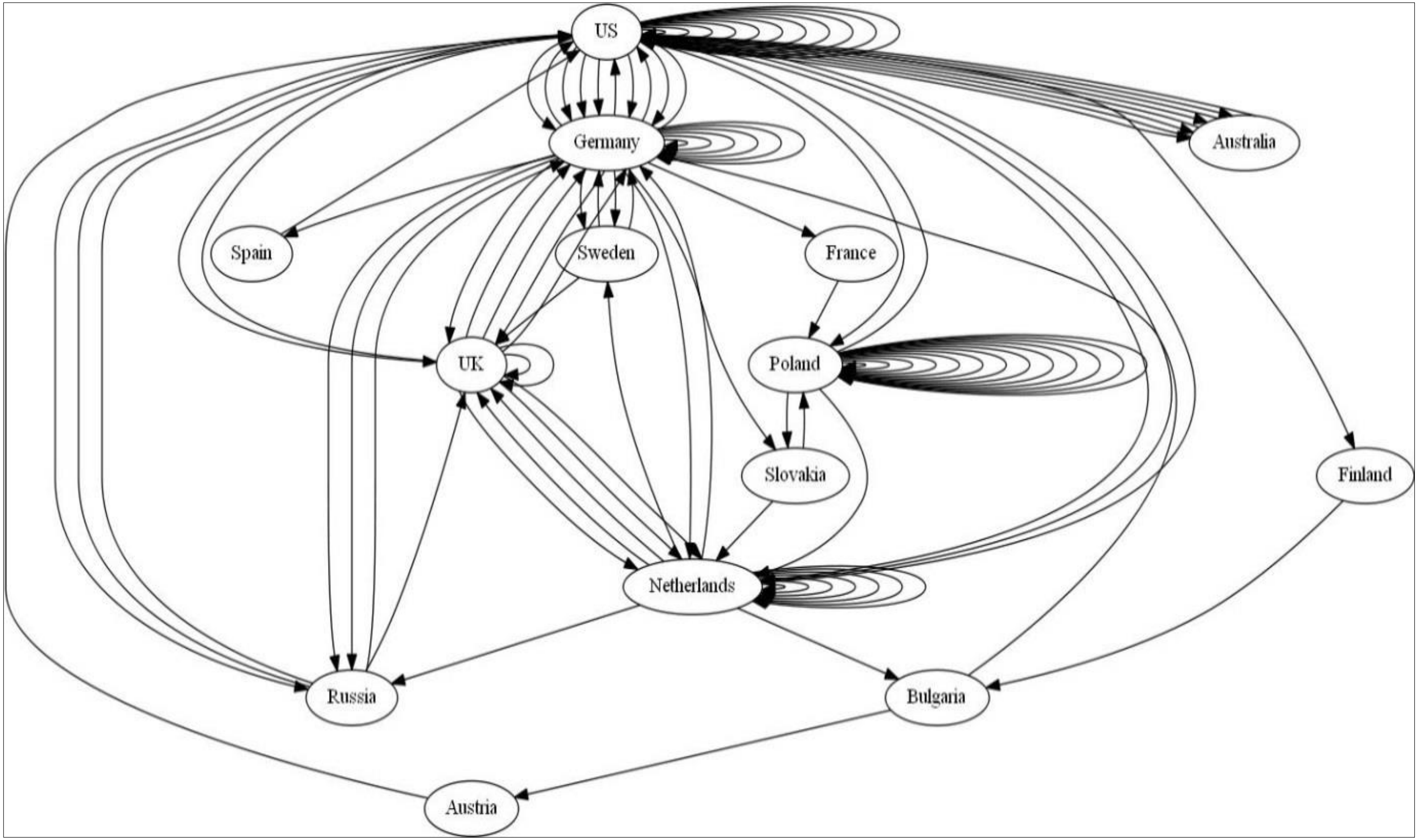
- US & Germany lead all others in terms of value and volume of transactions



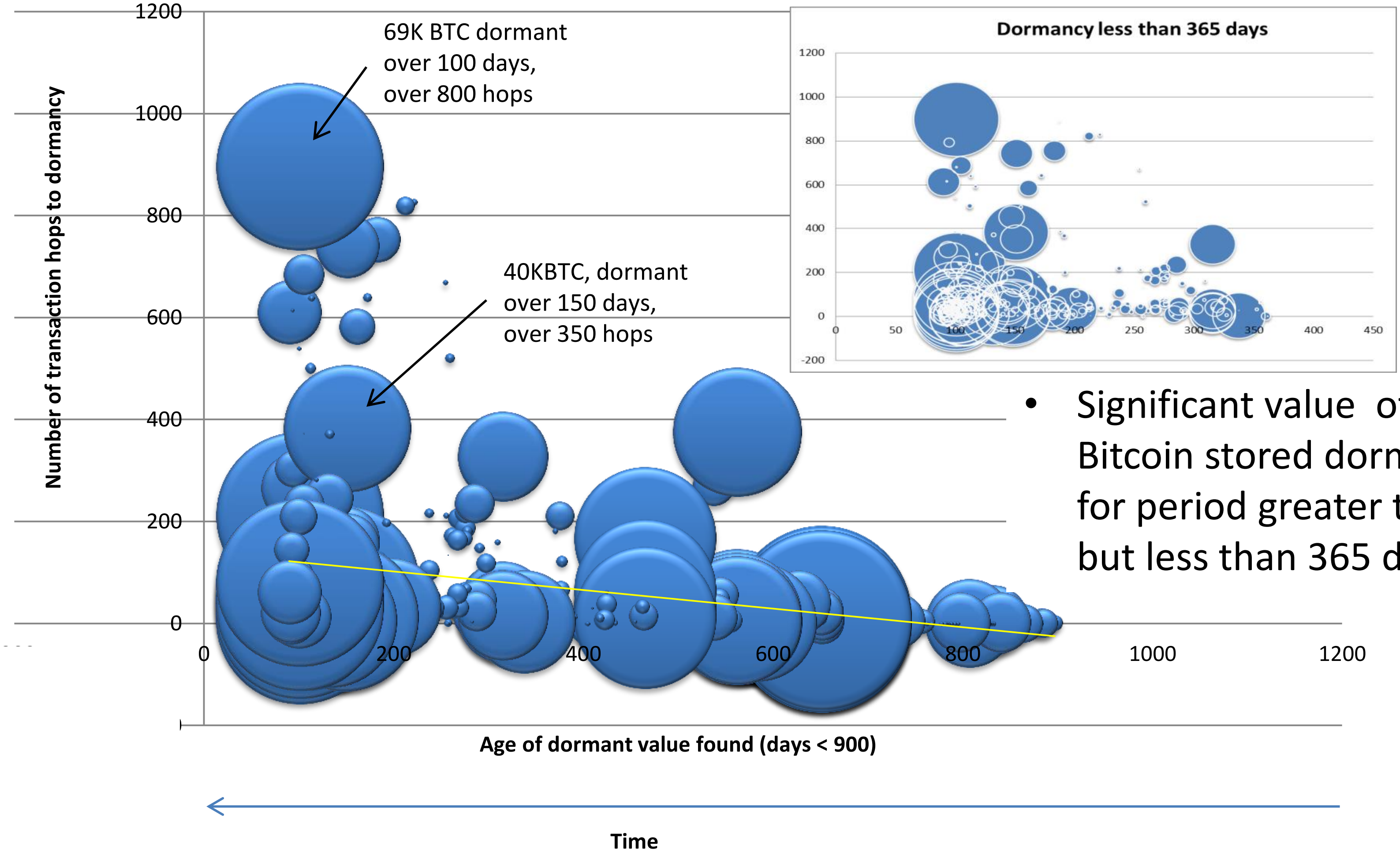
Initial Transaction Of 32K BTC ≈ $3.7M US Moves Over 240 Hours Decreasing By 36%



Initial Transaction Of 32K BTC ≈ $3.7M US Moves Over 240 Hours Decreasing By 36%



Quantities Of BTC In Individual Accounts Showing How Long They Have Been Dormant vs. Number Of Hops To Become Dormant



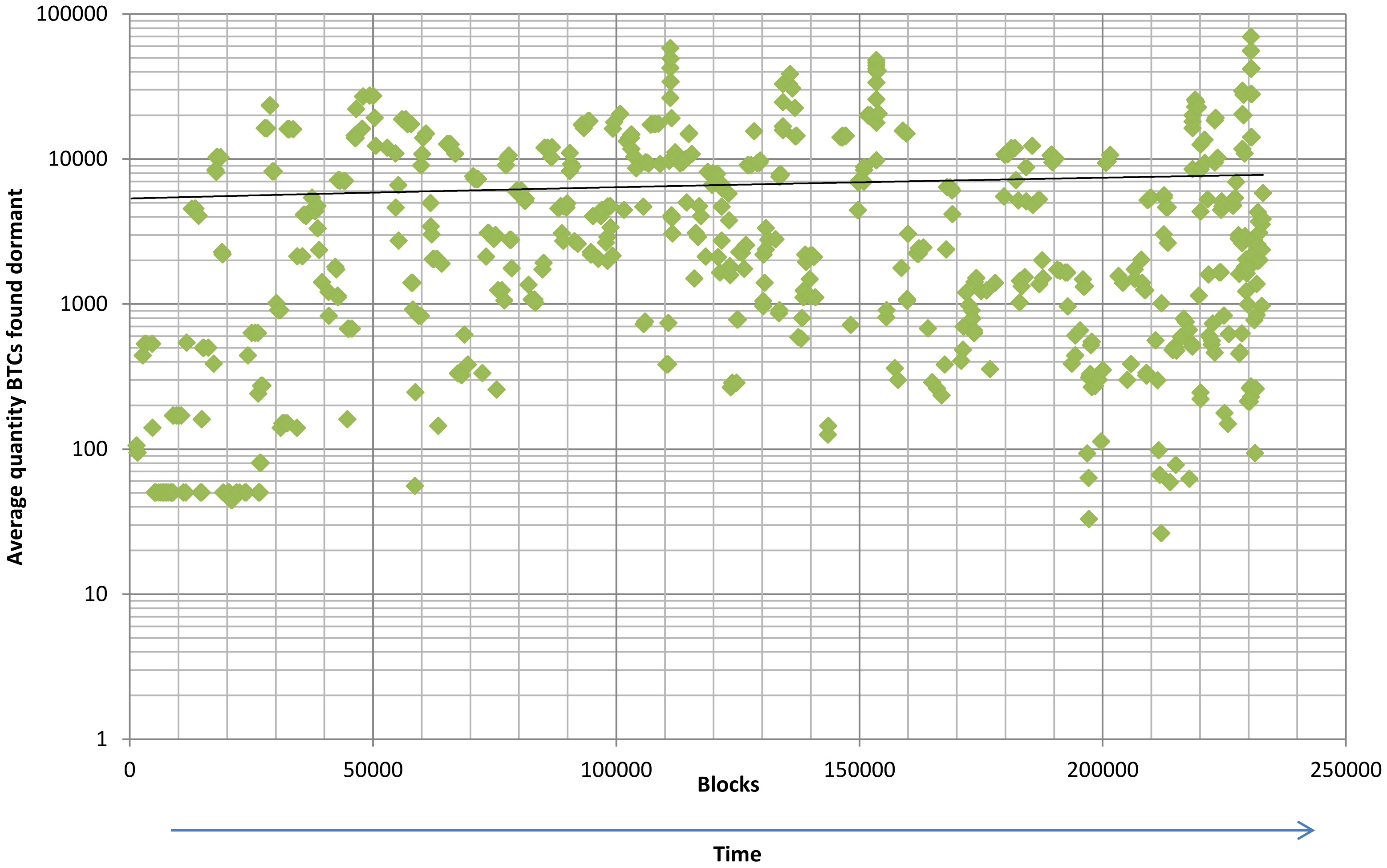
69K BTC dormant over 100 days, over 800 hops

40KBTC, dormant over 150 days, over 350 hops

- Significant value of Bitcoin stored dormant for period greater than 90 but less than 365 days

Indicating higher Average Number Of Hops before achieving dormancy In recent times

Graph Of Ordered Blocks Vs. Avg. Dormant Amount



The Average Quantity Of Dormant BTC (at a particular address) has been Increasing over time

Conclusion & Contribution

- Geographic patters of Bitcoin usage uncovered showing countries which have high volume of transactions and high value of transactions

- Complicated patterns revealed for high value Bitcoin transactions which seem to indicate attempts to annonymize transactions

- Average quantity of Bitcoin found dormant in addresses shows increase over time indicating increasing level of wealth being stored in Bitcoin

- Alternative methods to investigating and visualizing usage and geographic patterns can be used for Network Forensics and Investigative Finance

Future Works

- Examination of patterns of international transfers between pairs of countries to possibly reveal asymmetric flows