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, 1st August 2013

- 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 Bitcoin supply falls to zero over time

**2012**
- **Apr:** FBI paper on Bitcoin’s potential facilitating illicit activities
- **Oct:** ECB report classifies Bitcoin as virtual currency
- **Nov:** Miners’ reward (coinbase) halved to 25BTC

**2013**
- **Mar:** US: FinCEN guidelines encompassing aspects of Bitcoin ecosystem within their remit
- **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**
- **Aug:** 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
Examining The Blockchain And Constituent Transactions

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

http://www.javaworld.com/javaworld/jw-11-2011/Images/bitcoin2_fig1.png
Random Traversal Of Blockchain To Acquire Representative Sample Of Transactions

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

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

3) Get details from block’s coinbase transaction

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

5) Get IP address data from [http://blockchain.info](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.

- 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 anonymize 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.

![Pie chart showing IP address/country data analysis](chart.jpg)
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.
- 40K BTC, 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.
The Average Quantity Of Dormant BTC (at a particular address) has been increasing over time.
Conclusion & Contribution

• Geographic patterns 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 anonymize 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