# Stressing Out: Bitcoin "Stress Testing"

Khaled Baqer, Danny Yuxing Huang,
Damon McCoy and Nick Weaver

(given by Ross Anderson)

# Overview

- Spam attack on Bitcoin (July 2015)
- Importance: block size debate! At present you can bring down Bitcoin for $50k
- Goal here: highlight spam motifs, investigate impact, analyse security economics (fee income increase, cost of spam campaign)
- Used a clustering method to group transactions and find patterns

# Bitcoin spam

- **Fan-in**: Transactions that absorb a lot of inputs reduce the unspent transaction output (UTXO) set but still occupy substantial space in the blocks
- **Fan-out**: Transactions that split a few inputs into many outputs occupy space in blocks and also increase the UTXO set (Mempool impact)
- **Dust output**: “Dust” outputs convey a trivial amount of value but occupy the same amount of resources in the Bitcoin network

# Spam campaign (July 2015)

- Someone said, ‘stress testing Bitcoin network’
- Motivation (?): show Bitcoin is vulnerable to DoS, and get support to raise the block size
- DoS: send transactions with higher fees to deplete space in blocks
- Spam also uses many similar transactions to have a significant impact on the network
- But what does spam look like?

# *k*-means Clustering

**Table 2.** Transaction features

| Feature | Notation | Description |
|---|---|---|
| Inputs | $I$ | Number of inputs |
| Outputs | $O$ | Number of outputs |
| Ratio | $R$ | $I \div O$ |
| Priority | $P$ | Value-weighted measurement |
| Size | $S$ | Size (bytes) |
| Size and Ratio | $S \times R$ | Emphasize fan-in and fan-out |
| Fees | $F$ | Value of unclaimed outputs |
| Coin days destroyed | $CDD$ | Coin age and spending velocity |
| Value | $V$ | Total output value |
| Fees to values ratio | $F \div V$ | Emphasize fee differences |

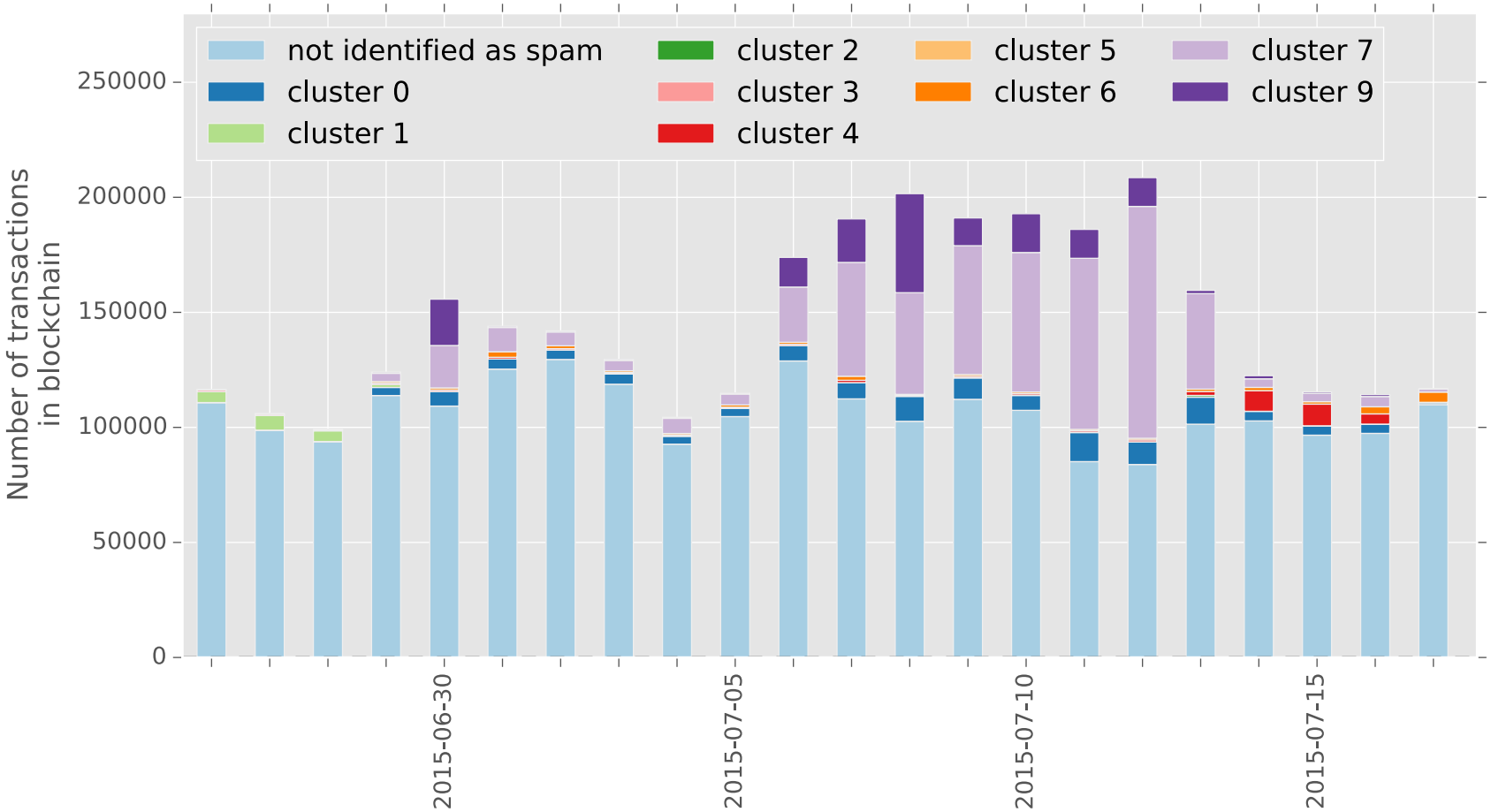
# *k*-means Clustering (II)

**Table 3.** Cluster centroids (*confirmed transactions*)

| *C* | *TXs* | *I* | *O* | *R* | *P* | *S* | *F* | *CDD* | *V* |
|---|---|---|---|---|---|---|---|---|---|
| 0 | 48K | 1.35 | 46 | 0.06 | 0.74 | 1.8K | 0.0004 | 0.195 | 4.06 |
| 1 | 28 | 4.4K | 1 | 4.4K | 0.001 | 645K | 0.04 | 0.06 | 0.0 |
| 2 | 896 | 106 | 1 | 103 | 0.17 | 16K | 0.001 | 0.34 | 0.13 |
| 3 | 20 | 1.1K | 1 | 1.1K | 0.0008 | 162K | 0.01 | 0.012 | 0.0 |
| 4 | 13.5K | 31 | 1 | 31 | 0.04 | 4.7K | 0.0002 | 0.02 | 0.006 |
| 5 | 16 | 1.4 | 13 | 0.15 | 535K | 668 | 0.0004 | 25K | 1K |
| 6 | 9.5K | 20 | 17 | 19 | 0.4 | 3.5K | 0.0004 | 0.14 | 1.4 |
| 7 | 425K | 1.1 | 2 | 0.8 | 1 | 224 | 0.0001 | 0.022 | 1.43 |
| 8 | 2 | 1 | 19 | 0.05 | 136M | 787 | 0.0002 | 740K | 3K |
| 9 | 117K | 1.2 | 11 | 0.14 | 72.43 | 561 | 0.0002 | 2.7 | 6.5 |

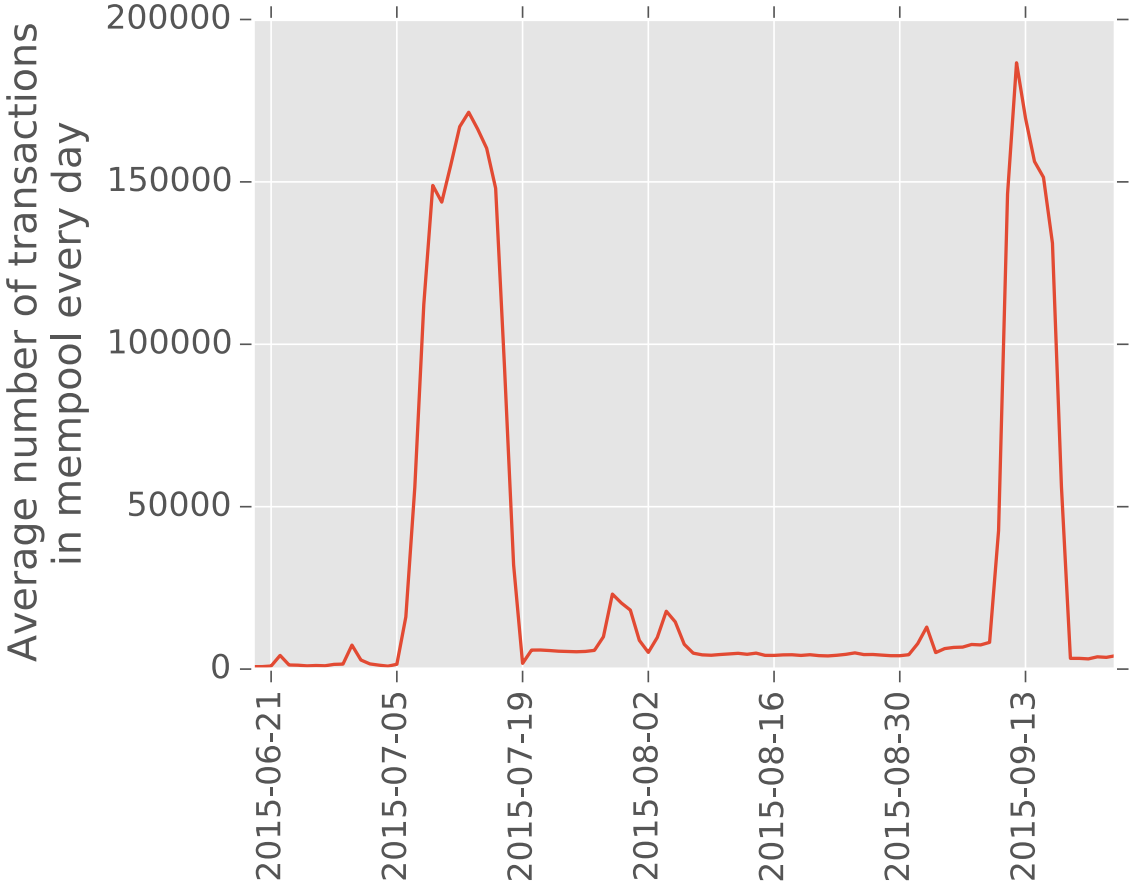
# Impact on Bitcoin:

## The number of transactions per day in the blockchain



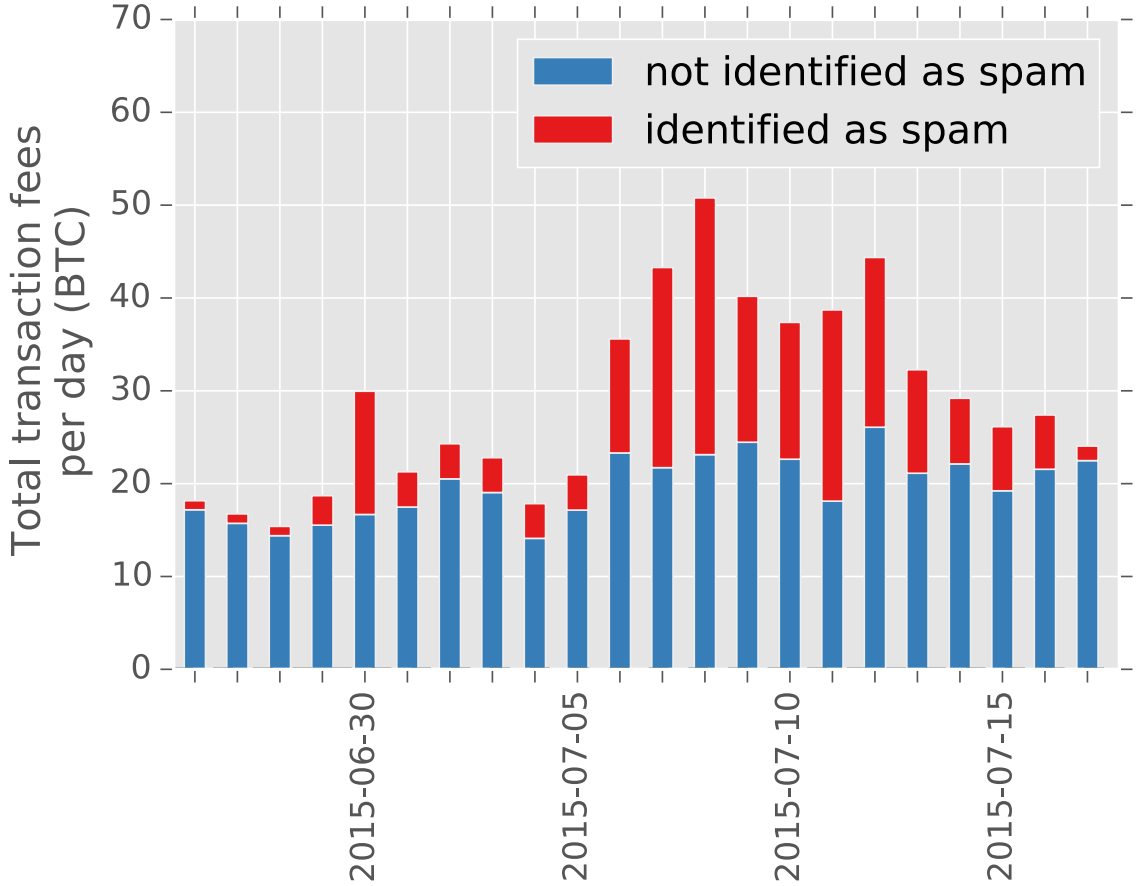
# Impact on Bitcoin (II):

## The average number of unconfirmed transactions



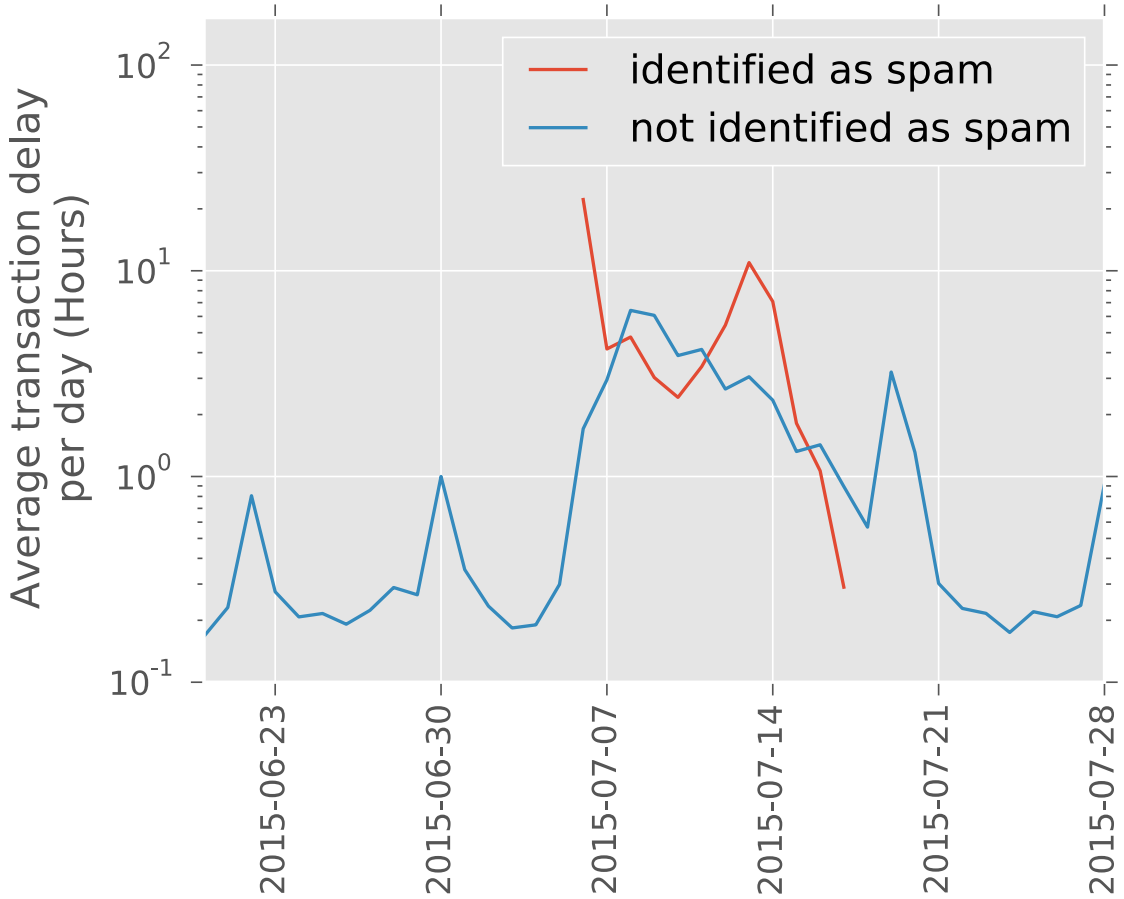
# Impact on Bitcoin (III):

## The total amount of transaction fees every day



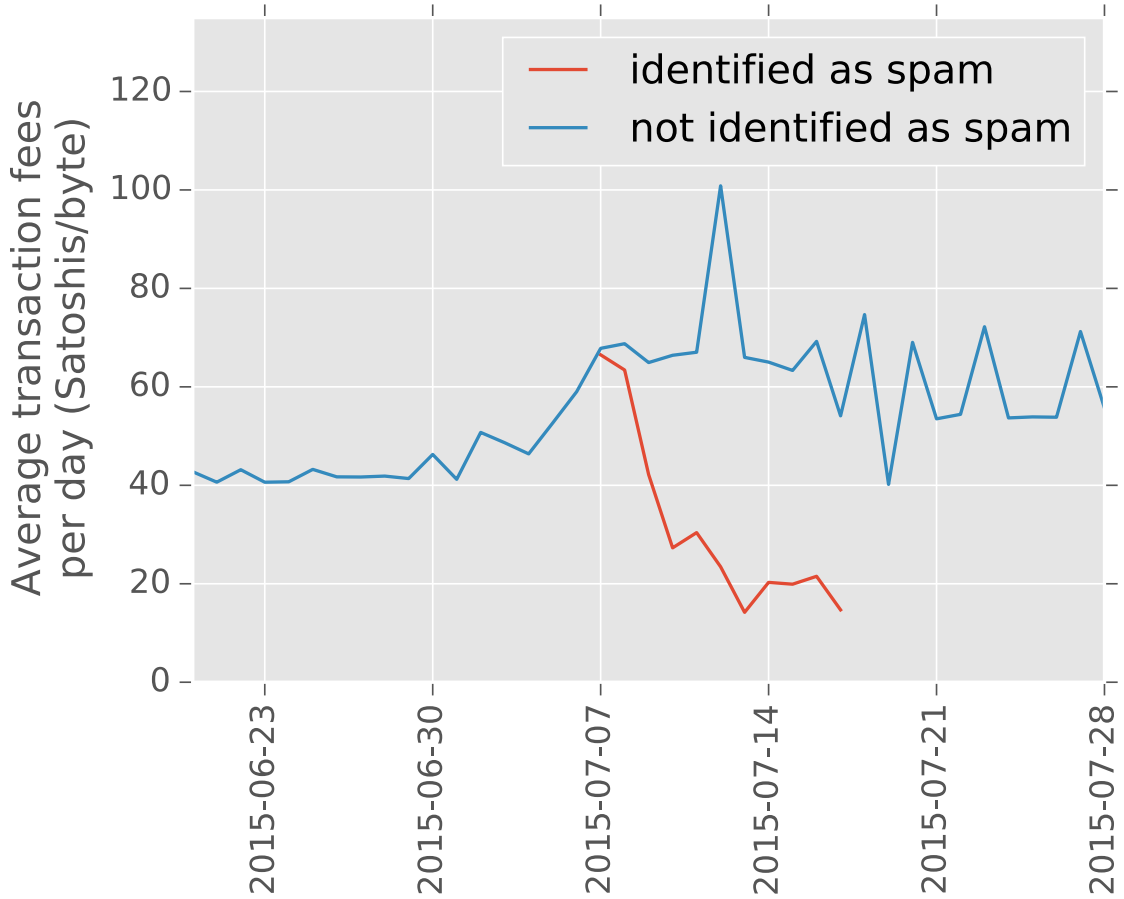
# Impact on Bitcoin (IV):

## Average transaction delay



# Impact on Bitcoin (V):

## Average transaction fees per transaction per day (normalized)



# Summary of results
(10-day spam campaign)

- 385,256 (23.41%) out of 1,645,667 total Bitcoin transactions were spam
- Spam increased average fees by 51% (from 45 to 68 Satoshis/byte)
- Spam increased processing delay by 7 times (from 0.33 to 2.67 hours)
- Cost of this attack on Bitcoin: $49K, about half being to pay higher fees

# Questions?

- If skype doesn't work,. email hard questions to khaled.baqer@cl.cam.ac.uk (who could not get a visa processed in time)
- Further possible discussions for the barbecue: sovereign risk and other emergent problems of governance