Univ of California San Diego
Computer Science and Engineering

BOTCOIN

Bitcoin-Mining on Botnets

Danny Y. Huang

Hitesh Dharmdasani, Sarah Meiklejohn
Vacha Dave, Chris Grier, Damon McCoy
Stefan Savage, Nicholas Weaver
Alex C. Snoeren, Kirill Levchenko

Motivation

Unique IP address → Money

Spam → $$$

Click-fraud → $$$

Computational Power → Money

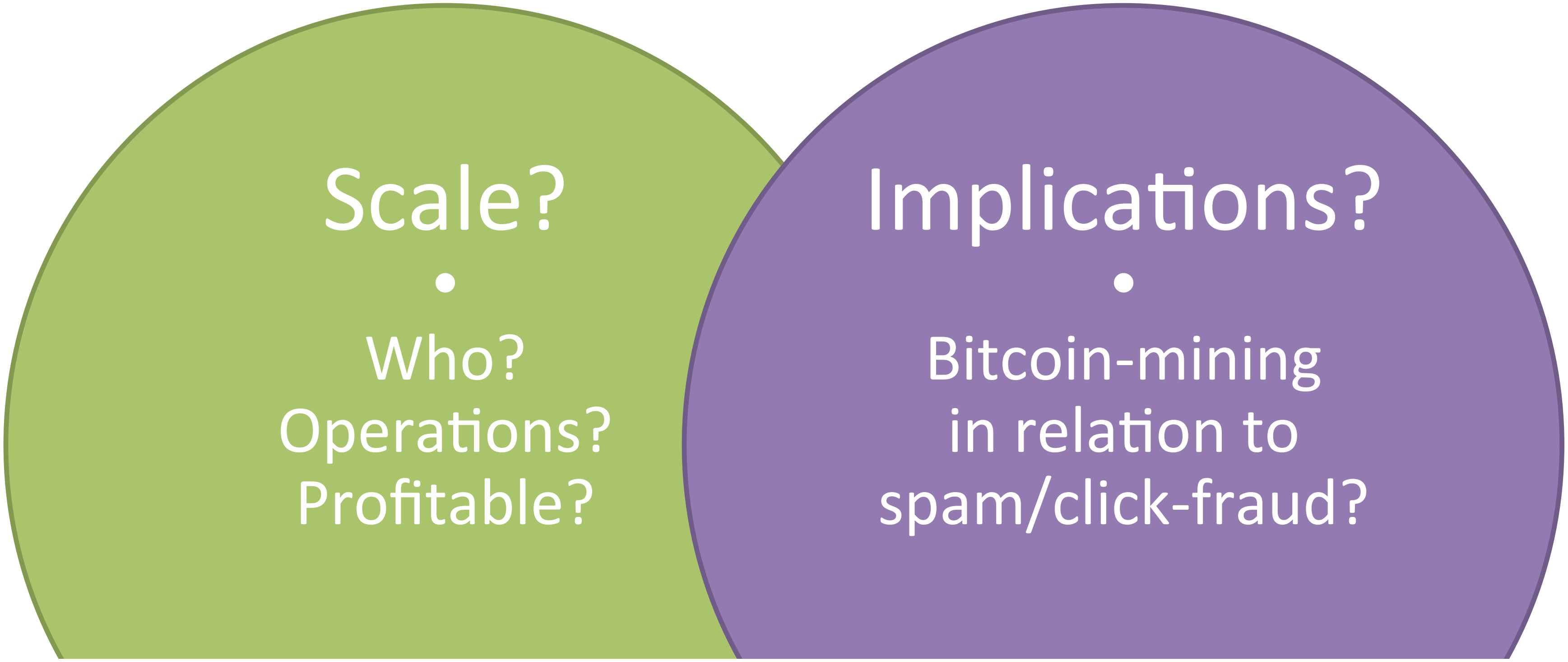
Mining Bitcoins → $$$

Motivation

Kevin

Loss in productivity

High electricity bill



Scale?

- Who?
  Operations?
  Profitable?

Implications?

- Bitcoin-mining
  in relation to
  spam/click-fraud?

Contributions

What we learned about botnets:

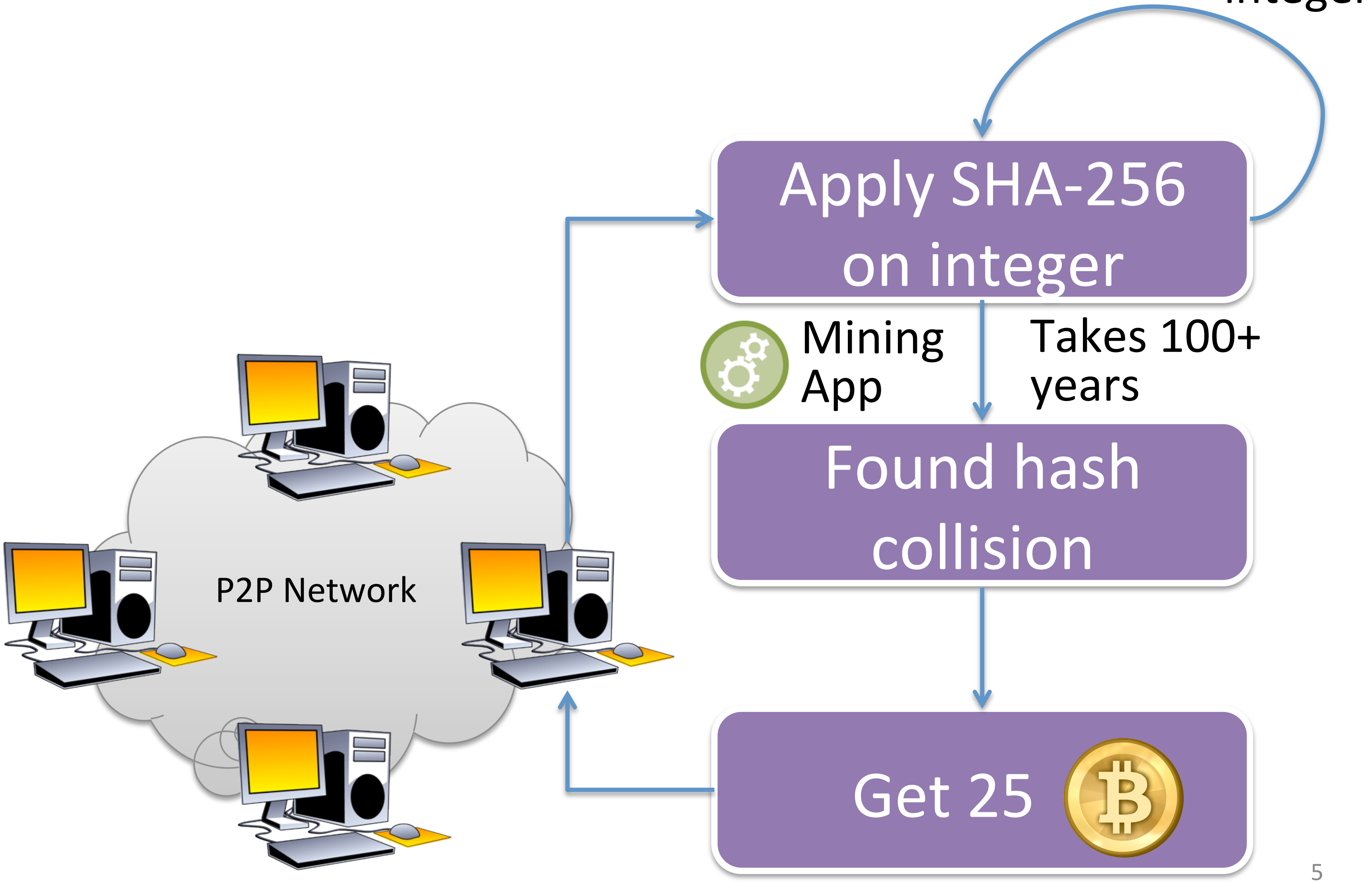
Identities

Modus Operandi

Revenue

Implications

How you can make bitcoins



Pick a different integer

Apply SHA-256 on integer

Mining App

Takes 100+ years

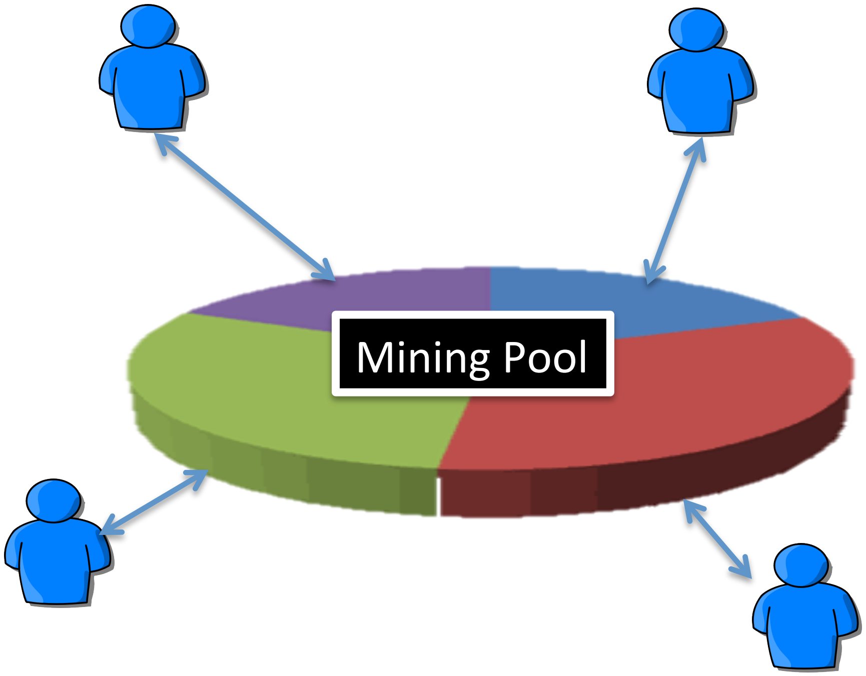
Found hash collision

Get 25

P2P Network

Mining Pools

- ❖ Parallelizes hashing.
- ❖ Finds solution faster.
- ❖ Workers divide reward.

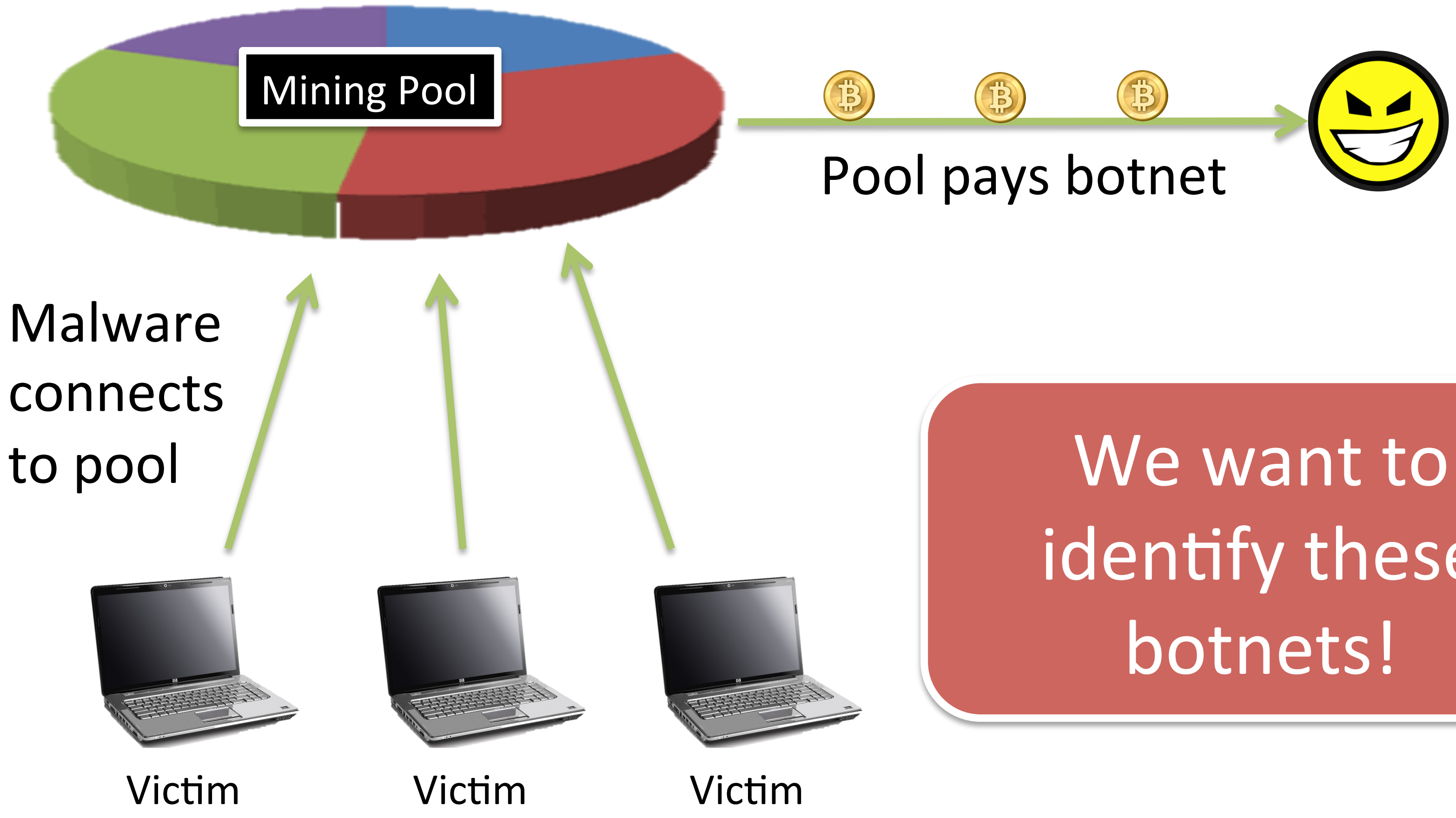


BUT:
Hardware costs
Energy costs

Free!

```
miner.exe my_wallet http://pool.com
```

Botnet Mining



Mining Pool

Pool pays botnet

Malware connects to pool

Victim

Victim

Victim

We want to identify these botnets!

```
miner.exe botnet_wallet http://pool.com
```

Finding the Mining Malware

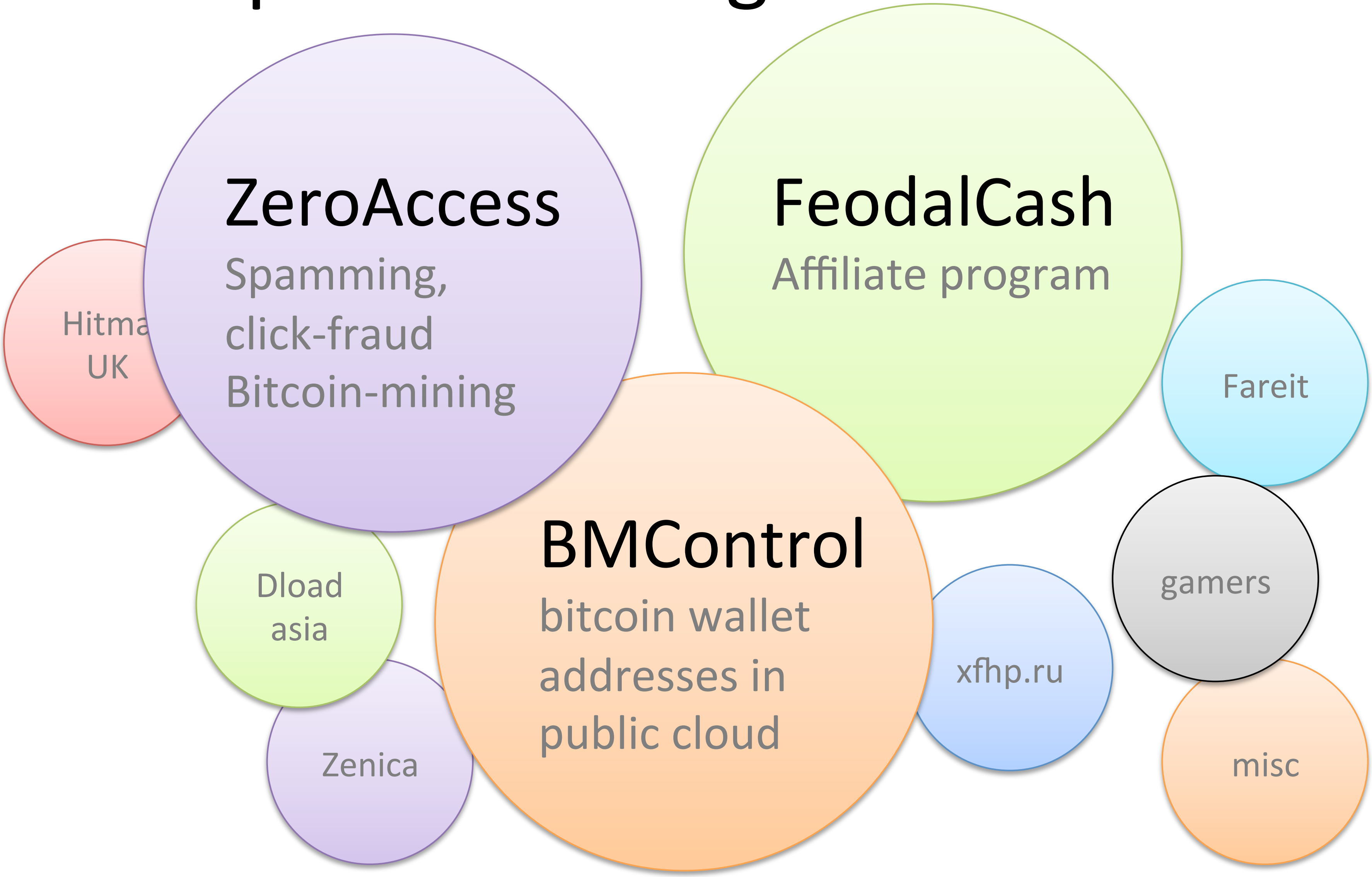
2,000 binaries
10 botnets

Malware Databases
Threat Expert, Emerging Threats, …

Bitcoin Malware
Reports / Blogs

Leaked Data
Interviews with Pools

Examples of Mining Botnets



ZeroAccess

Spamming,
click-fraud
Bitcoin-mining

FeodalCash

Affiliate program

BMControl

bitcoin wallet
addresses in
public cloud

Hitma
UK

Dload
asia

Zenica

xfhp.ru

Fareit

gamers

misc

Outline

What we learned about botnets:

Identities

2,000 binaries
10 botnets

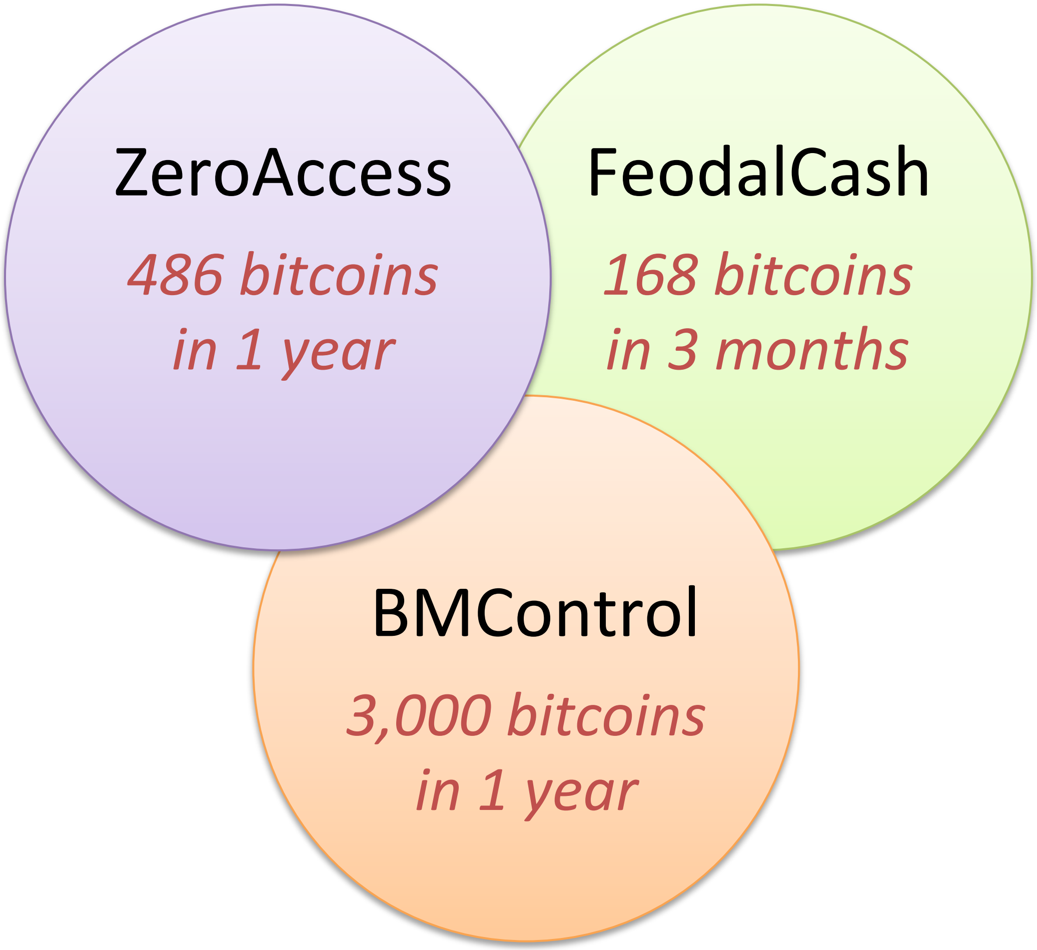
Modus Operandi

e.g. affiliate program,
wallet addresses in cloud

Revenue

Implications

Botnet Mining Revenue



ZeroAccess

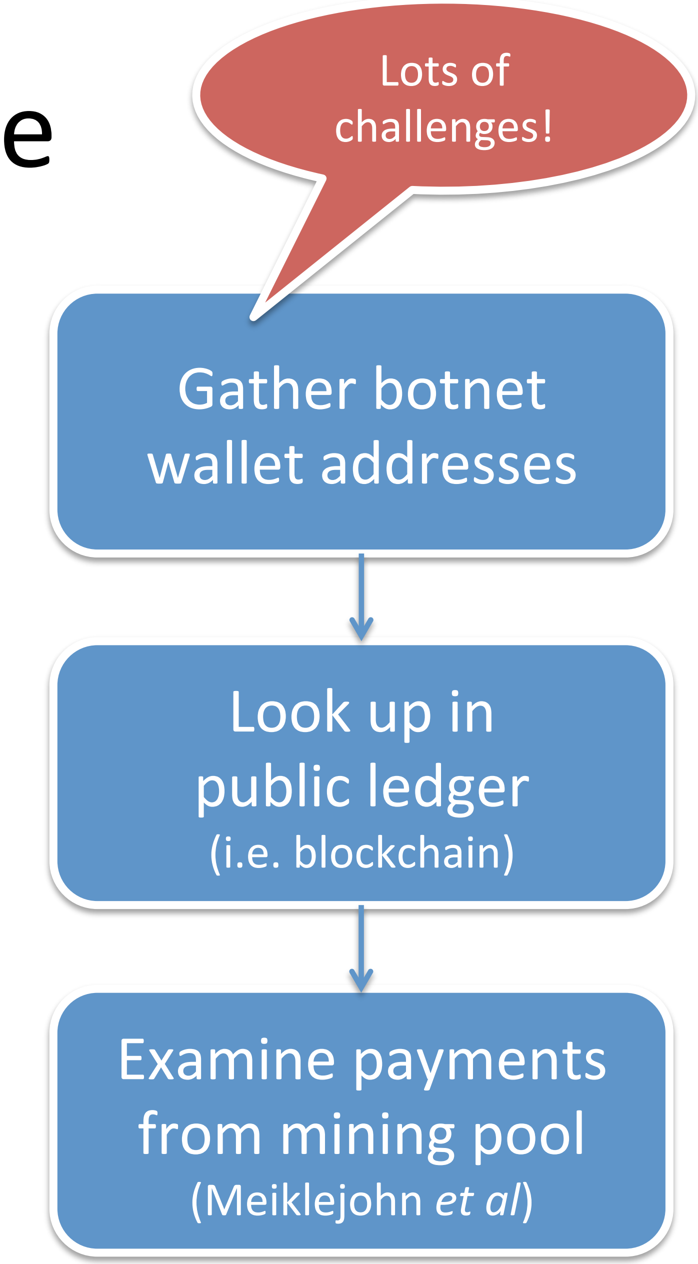
486 bitcoins in 1 year

FeodalCash

168 bitcoins in 3 months

BMControl

3,000 bitcoins in 1 year



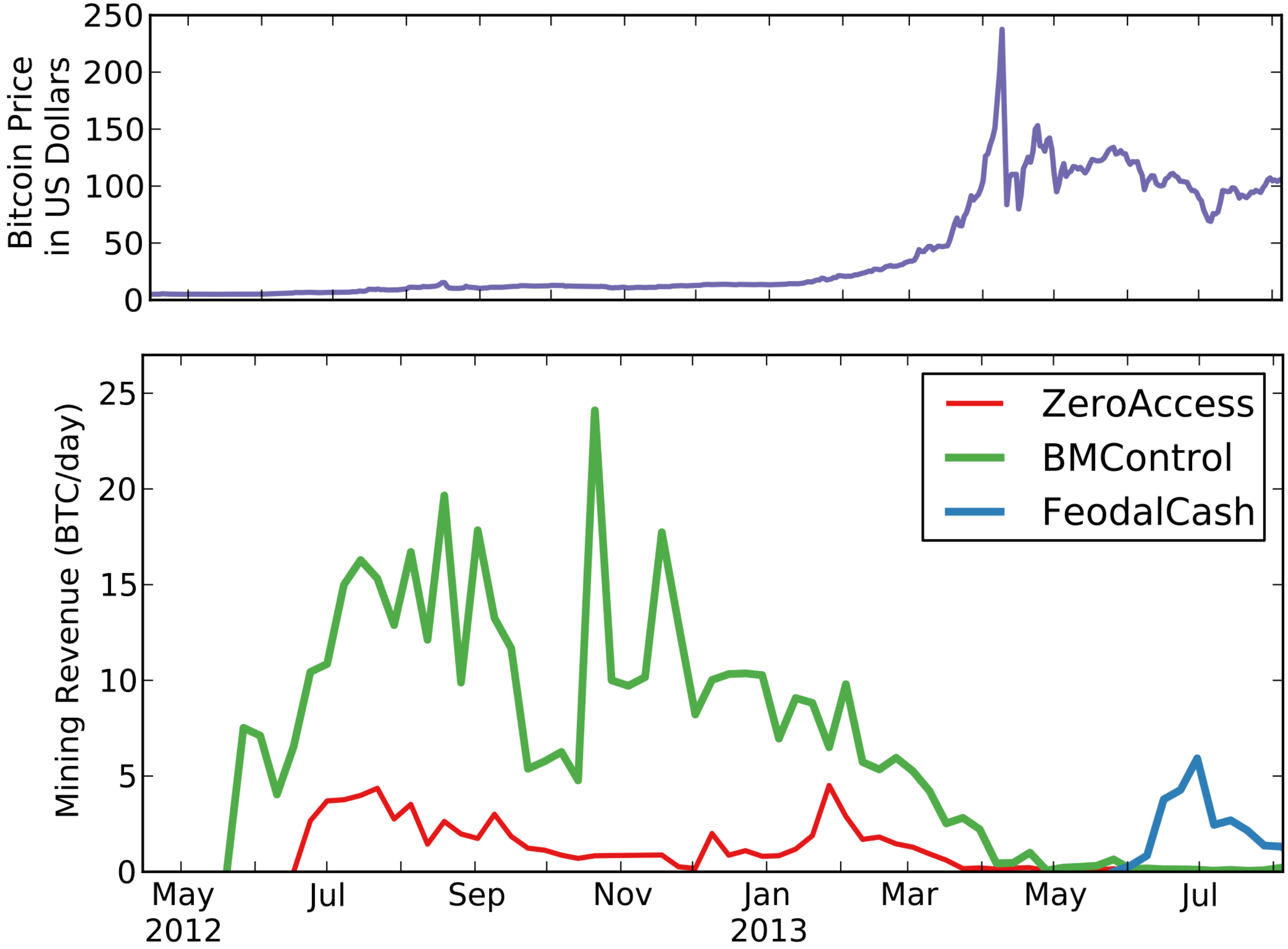
Lots of challenges!

Gather botnet wallet addresses

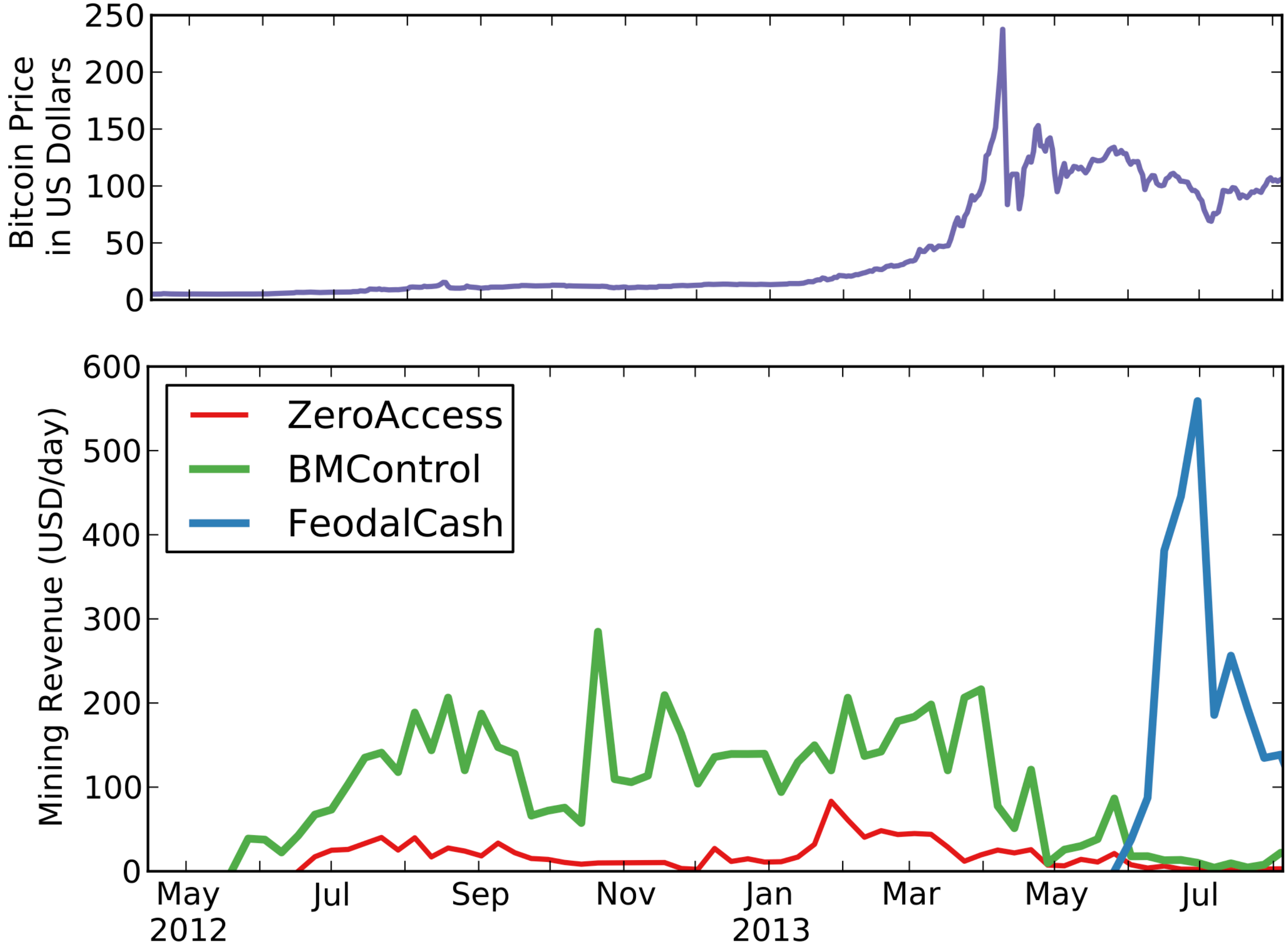
Look up in public ledger (i.e. blockchain)

Examine payments from mining pool (Meiklejohn *et al*)

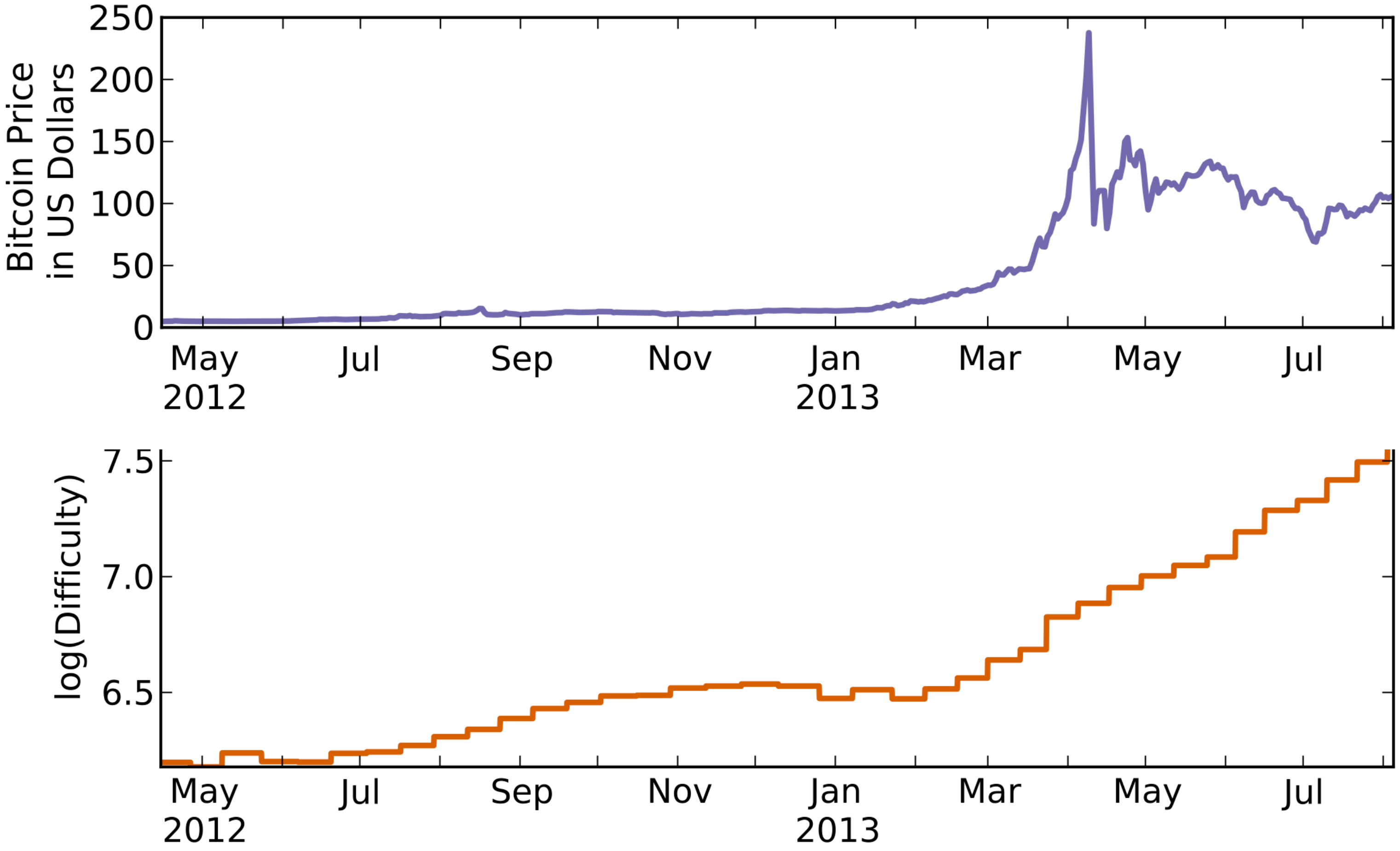
Botnet Revenue in Bitcoins



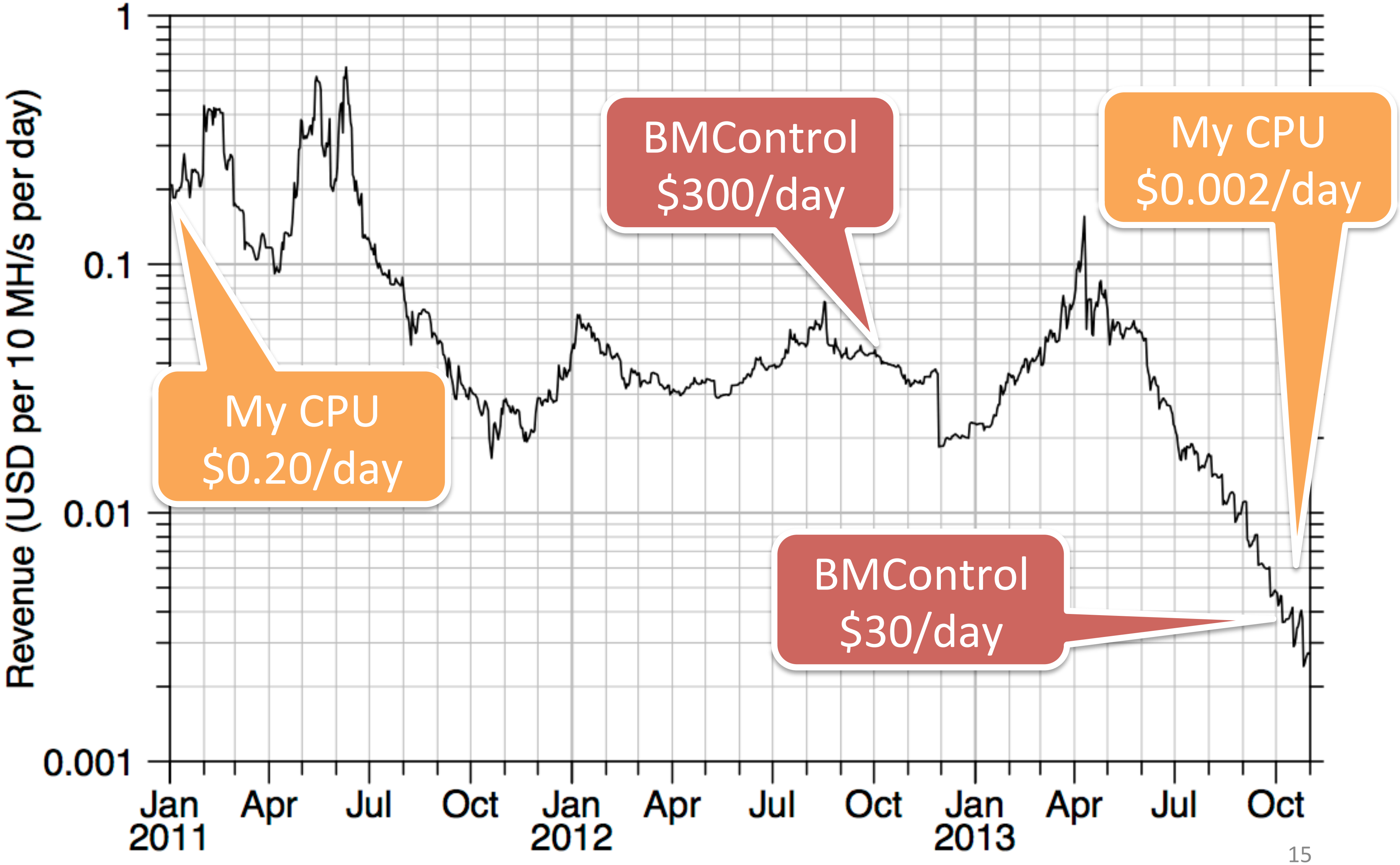
Botnet Revenue in US Dollars



Mining Revenue



Mining Revenue



BMControl
$300/day

My CPU
$0.002/day

My CPU
$0.20/day

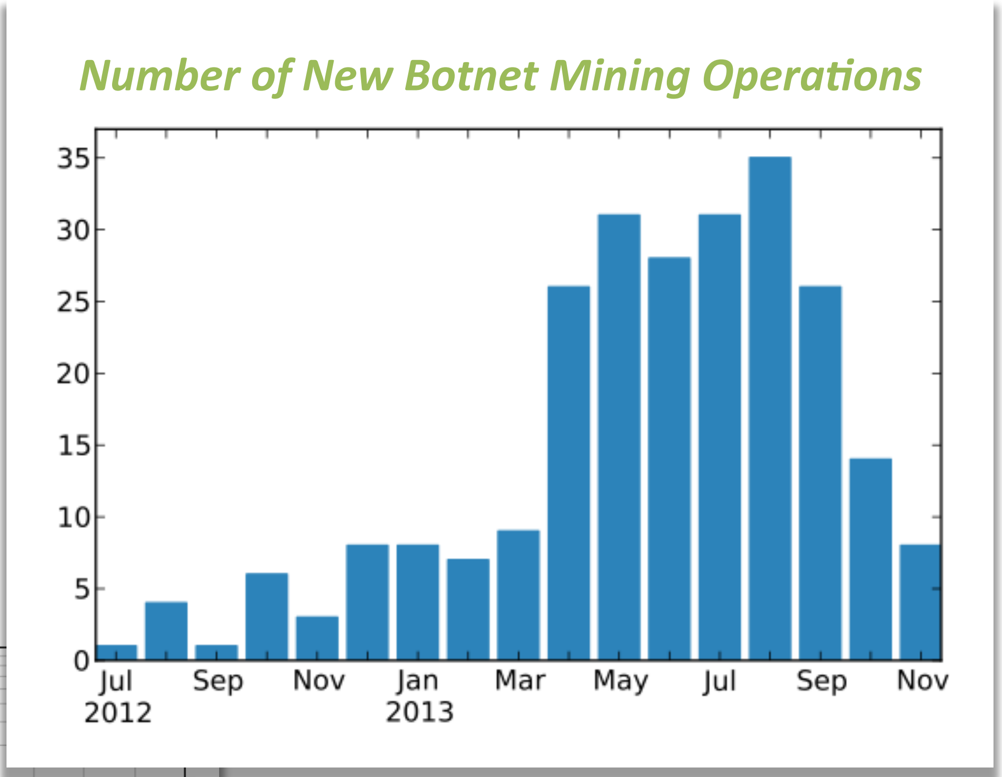
BMControl
$30/day

Litecoin Mining

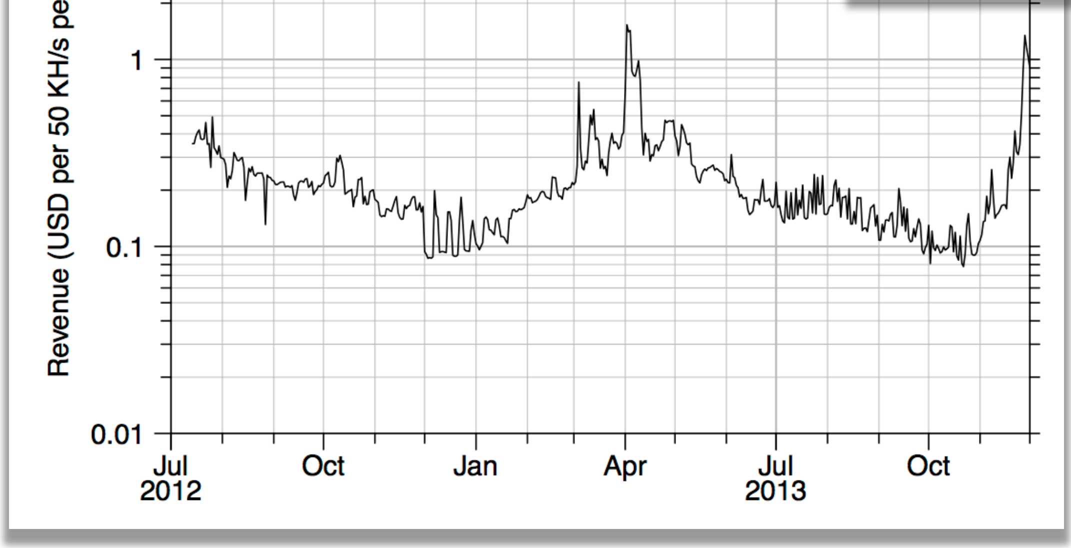
Different hash function

- Bitcoin: SHA-256
- Litecoin: Scrypt

Number of New Botnet Mining Operations



Litecoin Mining Revenue



Outline

What we learned about botnets:

Identities

2,000 binaries
10 botnets

Modus Operandi

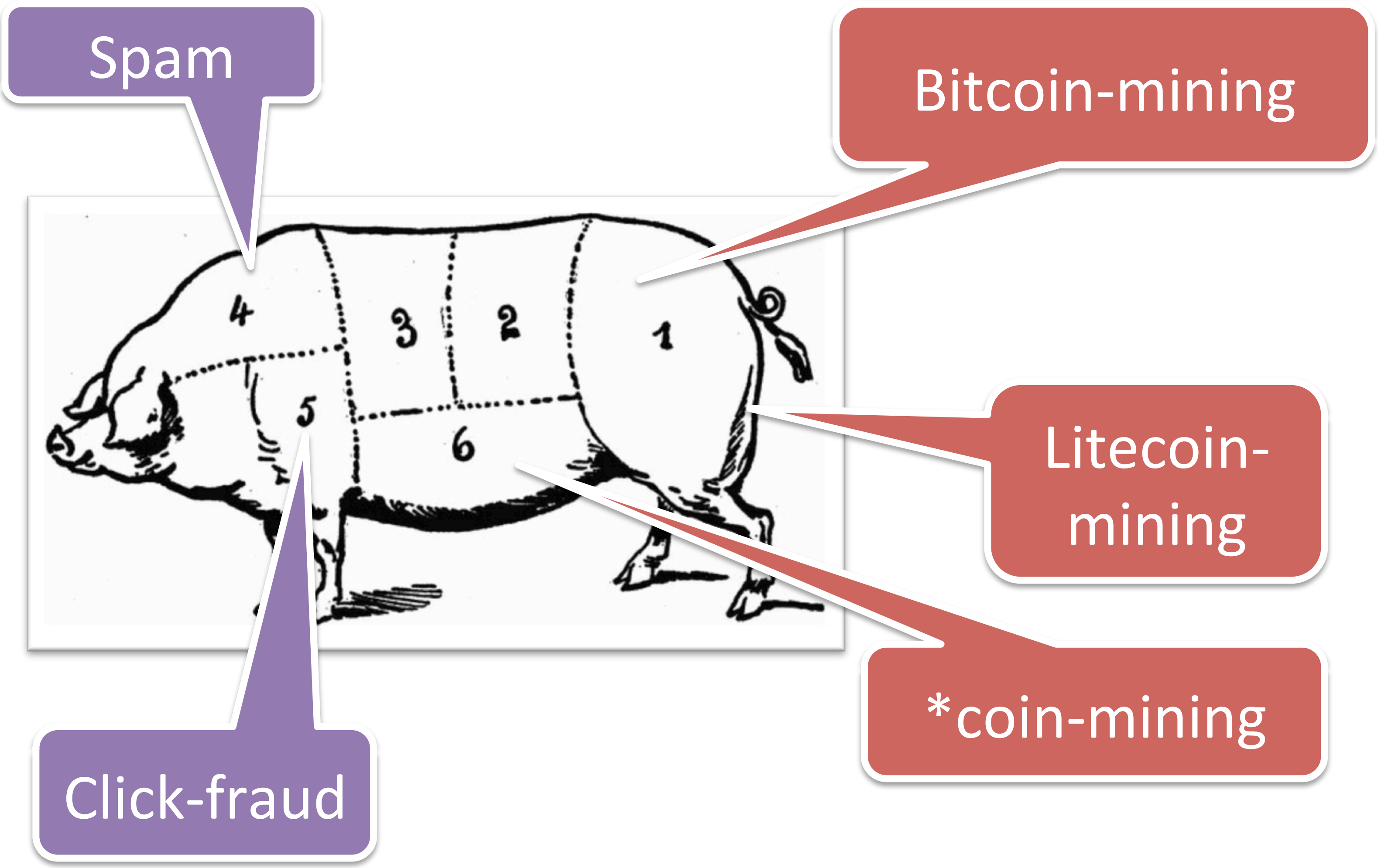
e.g. affiliate program,
wallet addresses in cloud

Revenue

4,000 bitcoins
in 2 years

Implications

Implication & Conclusion



Spam

Bitcoin-mining

Litecoin-mining

*coin-mining

Click-fraud

Outline

What we learned about botnets:

Identities

Modus Operandi

Revenue

Implications