Bots and Bitcoin

Hitesh Dharmdasani
George Mason University
Agenda

0 What is bitcoin?
0 Bots
0 What makes bitcoin special
0 The evolution of GPUs and ASICS
0 Intricacies of bitcoin
0 Pooled Mining
0 How are bitcoins made by bots
0 Situation today
Bitcoins

- Decentralized crypto currency
- Does not exist in tangible form
- Kept in wallets
- Accounts identified via payout addresses
- Spend resources = get bitcoins
1 BTC = 31.95473 USD
Bots

- Compromised Computers performing computations
- Infection vectors are many
- Pay per install is most efficient
What makes bitcoin special

• Currency is valid across boundaries
• Defined by a chain of signatures. Blocks
• Anonymous behavior
  • Don’t know who sends money to whom
Tech Spec for Bitcoin

0 A database shared by all nodes in the bitcoin network has all the transactions. Called the blockchain
0 Every block contains the hash of the previous block
0 Once verified, Transactions are appended to blocks
0 Proof-of-work guarantees the faith in the transaction
0 When a new block is created. A special transaction called the coinbase transaction is added to the blockchain. Notifying the miner of the block with his reward
The evolution of GPUs and ASICs

0 GPUs are made to perform fast integer and floating point calculations
0 Have many cores. Sometimes upto 250
0 Perfect for generating hashes in parallel
0 Application Specific Integrated Circuits (ASICs) are even better.
The Popular and *mythicizing*

<table>
<thead>
<tr>
<th></th>
<th>Price</th>
<th>Unit</th>
<th>Capacity</th>
<th>PCH</th>
<th>Power</th>
<th>Efficiency</th>
</tr>
</thead>
<tbody>
<tr>
<td>BitForce Single SC</td>
<td>$1,299.00</td>
<td>Unreleased</td>
<td>60000</td>
<td>60</td>
<td>46.1894</td>
<td>1000</td>
</tr>
<tr>
<td>BitForce Jalapeno</td>
<td>$149.00</td>
<td>Unreleased</td>
<td>4500</td>
<td>4.5</td>
<td>30.2013</td>
<td>1000</td>
</tr>
<tr>
<td>ATI Radeon 5830</td>
<td>$239.00</td>
<td>$70.00</td>
<td>220</td>
<td>130</td>
<td>3.1429</td>
<td>1.69</td>
</tr>
<tr>
<td>ATI Radeon 5870</td>
<td>$379.00</td>
<td>$140.00</td>
<td>420</td>
<td>190</td>
<td>3.0000</td>
<td>2.21</td>
</tr>
<tr>
<td>ATI Radeon 6950</td>
<td>$299.00</td>
<td>$125.00</td>
<td>350</td>
<td>150</td>
<td>2.8000</td>
<td>2.33</td>
</tr>
<tr>
<td>ATI Radeon 5850</td>
<td>$259.00</td>
<td>$99.00</td>
<td>270</td>
<td>150</td>
<td>2.7273</td>
<td>1.80</td>
</tr>
<tr>
<td>ATI Radeon 5970</td>
<td>$599.00</td>
<td>$289.00</td>
<td>700</td>
<td>325</td>
<td>2.4221</td>
<td>2.15</td>
</tr>
<tr>
<td>ATI Radeon 6970</td>
<td>$369.00</td>
<td>$199.00</td>
<td>400</td>
<td>200</td>
<td>2.0101</td>
<td>2.00</td>
</tr>
<tr>
<td>BitForce MiniRig (FPGA)</td>
<td>$15,295.00</td>
<td>$15,295.00</td>
<td>25200</td>
<td>1250</td>
<td>1.6476</td>
<td>20.16</td>
</tr>
<tr>
<td>ATI Radeon 7970</td>
<td>$550.00</td>
<td>$375.00</td>
<td>600</td>
<td>350</td>
<td>1.6000</td>
<td>1.71</td>
</tr>
<tr>
<td>ATI Radeon 7950</td>
<td>$450.00</td>
<td>$289.00</td>
<td>450</td>
<td>300</td>
<td>1.5571</td>
<td>1.50</td>
</tr>
<tr>
<td>ATI Radeon 6990</td>
<td>$950.00</td>
<td>$500.00</td>
<td>700</td>
<td>300</td>
<td>1.4000</td>
<td>2.33</td>
</tr>
<tr>
<td>BitForce Single (FPGA)</td>
<td>$599.00</td>
<td>$599.00</td>
<td>832</td>
<td>80</td>
<td>1.3890</td>
<td>10.40</td>
</tr>
<tr>
<td>nVidia GeForce GTX</td>
<td>$499.00</td>
<td>$450.00</td>
<td>200</td>
<td>200</td>
<td>0.6333</td>
<td>0.02</td>
</tr>
</tbody>
</table>
### In perspective

<table>
<thead>
<tr>
<th>Hash Rate</th>
<th>Daily Earnings</th>
<th>Time to mine a block</th>
</tr>
</thead>
<tbody>
<tr>
<td>AMD CPU@15 MH/s</td>
<td>$0.07</td>
<td>~ 33 Years</td>
</tr>
<tr>
<td>AMD GPU 5850x6 @ 2135 MH/s</td>
<td>$9.28</td>
<td>~ 85 days</td>
</tr>
<tr>
<td>Avalon ASIC @ 66300 MH/s</td>
<td>$288.13</td>
<td>~ 3 days</td>
</tr>
</tbody>
</table>

Current reward for mining a block is 25 BTC -> $777
Pooled Mining

0 Leverages on ‘divide and conquer’
0 Makes the larger proof of work into smaller proof-of-work problems
0 Every node can be given a space to enumerate hashes and submit.
0 Reward is paid daily. Even if it is 0.01 BTC
0 The existing miner programs work here. Just on artificial difficulty levels.
Pooled Mining 2

0 Good pools and bad pools
0 With pools. It’s a race to the finish
0 Whoever submits the proof-of-work first. Wins!
0 Reward is only on solving proof-of-work. Not to confirm the proof-of-work
0 pool.dload.asia – currently known to be mining. And a small bunch of .ru domains
Botnets making bitcoins

- Think of 5 MH/s per CPU
- For a botnet with 100,000 hosts.
- Total CPU hashing power is 500,000 MH/s
- At the current difficulty. That turns out to $2250 a day. Plus a block reward every 11 hours.
- Close to $3700 in 24 hours.
- You don’t even have to own the botnet. You can rent it!
Mining is said to be happening in the wild.

Symantec has reported as early as 2010 that botnet mining could be a possibility.

There is malware known to contact bad pools for mining.

Sophos has shown that the Zero Access botnet is known for bitmining.

Guessing a bad pool

0 The problem at hand
0 Malware owners and writers have their own pool
0 How to find out how much money was made by using a botnet
0 Cant find unless you mine a block using malware.
0 Reversing merkel roots of a tree of blocks to find variations in the coinbase transaction
0 Not fast unless amazon is your best bud
Interesting Trivia

0 The hard limit for bitcoins is 21 Million BTC
  0 Does this mean that bitcoin will be treasured later?
  0 Or will it just fail when people lose trust in a digital signature? Or computing power is so high that you can break the very premise of blocks?
  0 Ponzi Scheme?

0 The smallest unit in a bitcoin is 1 satoshi which is equivalent to 0.00000001 BTC

0 Mt Gox is currently one of the biggest exchanges to convert BTC to USD.
Questions

0 Slides on
http://mason.gmu.edu/~hdharmda/bitcoin.pdf

If you have an ASIC. And want to mine. Let me know ;)