Bots and Bitcoin

Hitesh Dharmdasani
George Mason University

Agenda

- What is bitcoin?
- Bots
- What makes bitcoin special
- The evolution of GPUs and ASICs
- Intricacies of bitcoin
- Pooled Mining
- How are bitcoins made by bots
- 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

- A database shared by all nodes in the bitcoin network has all the transactions. Called the blockchain
- Every block contains the hash of the previous block
- Once verified, Transactions are appended to blocks
- Proof-of-work guarantees the faith in the transaction
- 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

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

The Popular and *mythicizing*

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

In perspective

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

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

Pooled Mining

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

Pooled Mining 2

- Good pools and bad pools
- With pools. It's a race to the finish
- Whoever submits the proof-of-work first. Wins!
- Reward is only on solving proof-of-work. Not to confirm the proof-of-work
- 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!

More botnets

- 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. http://www.sophos.com/en-us/why-sophos/our-people/technical-papers/zeroaccess-botnet.aspx

Guessing a bad pool

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

Interesting Trivia

- The hard limit for bitcoins is 21 Million BTC
  - Does this mean that bitcoin will be treasured later?
  - 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?
  - Ponzi Scheme?
- The smallest unit in a bitcoin is 1 satoshi which is equivalent to 0.00000001 BTC
- Mt Gox is currently one of the biggest exchanges to convert BTC to USD.

Questions

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

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