# **Brief Tutorial on Bitcoins**

Abde Ali Kagalwalla

NanoCAD Lab



# What is Bitcoin ?



- Protocol to manage digital currency and process payments between users
- First proposed by "Satoshi Nakamoto"
- No central authority (Federal Reserve) or banks to manage transactions
- Decentralized, P2P system



NanoCAD Lab



# Valuation of bitcoin

Market Price (USD) Source: blockchain.info



NanoCAD Lab

puneet@ee.ucla.edu



# Digital Signature (Image Source: Wikepedia)





If the hashes are equal, the signature is valid.

### NanoCAD Lab

#### puneet@ee.ucla.edu



# **Bitcoin Transactions via Digital Signature**



- Online transactions currently verified by a bank
  - Does Abde Ali own enough bitcoins ?
  - Double spending: Abde Ali should not be able to use the same bitcoins to pay Weiche
- Can a bank be completely eliminated from the online payment transfer protocol ?
  - $\rightarrow$  Ingenuity of Bitcoin



### Decentralized Transaction Verification: Block Chain

- Public ledger of transactions
- A set of transactions referred to as a 'block'
- All verified blocks are added to the global block chain
- Liangzhen can look at the block chain and check if Abde Ali is not cheating
- Problem: What if Abde Ali tries to pay both Liangzhen and Weiche at the same time ?



UCLA

#### puneet@ee.ucla.edu

### NanoCAD Lab

### Prevent Double Spending: Computationally Intensive Verification

- Potential Solution: Both Liangzhen and Weiche publicly release the digital message and request all users to verify
- Problem: Abde Ali can create millions of users that will validate both transactions
- Bitcoin solution is to make verification computationally expensive using a proof-of-work protocol
  - Solve a artificially challenging puzzle to verify a block chain
  - Reward users who verify blocks with new 'mined' bitcoins
  - This verification is done by bitcoin miners



### Bitcoin Mining Challenge Puzzle: Proofof-Work



- Since hash function is 'almost' random, 2<sup>K</sup> attempts are required to solve the challenge
- On average blocks are verified in 10 minutes
- The successful miner is rewarded with 25 newly generated bitcoins
  - Number of bitcoins generated will be halved after every 210,000 validated blocks
  - Bitcoin generation will stop once the reward less than 10<sup>-8</sup> (Minimum unit called Satoshi)
  - Miners also receive transaction fees



# **Bitcoin Mining Infrastructure**

- Initially Satoshi's open source software could be used on any CPU → No longer viable
- GPU and FPGA based mining is fairly popular
- ASIC solutions are the most viable option now

	Spartan6-150	BFL Single	BFL miniRig	Avalon	BFL	ASICminer
Туре	Xilinx FPGA	Altera FPGA	FPGA	ASIC	ASIC	ASIC
Process	45 nm	45 nm (?)	45 nm (?)	110 nm	65 nm	130 nm
Hash Rate Per Chip	210 MH/s	415 MH/s	650-750 MH/s	280 MH/s	4 GH/s	300 MH/s
Power Draw	15 W	40 W	35 W	2.8 W	30 W	2.5 W
Efficiency (MH/s per W)	14	10	20	100	133	120
US\$ / MH/s	1 to 2.5	0.75	0.6	Varies	Varies	Varies
Notes	Typically 1 to 4 FPGAs Per Board	2 FPGAs Per Board	2 FPGAs Per Board, 17 to 18 Boards	Priced In BTC (prices increase)	BFL Anticipates A Slight Reduction In Power Draw	Priced In BTC (prices increase)

### **Comparison of FPGA and ASIC Chips**

### NanoCAD Lab

puneet@ee.ucla.edu



### Comparison of Bitcoin Mining Hardware:https://bitcoinwisdom.com/bitcoin/cal culator

Velocity location         CONTRACT         Contract <thcontract< th="">         Contract         Contract</thcontract<>	+													
Nume & ET TITLES         OPENNEW           Difficulty increment: (?)         5           Electricity Price: (USD/W/h)         0.1           Pool Fee:         2           2         5           Handbranz Price: (USD/W/h)         0.1           Pool Fee:         2           1         448/Fast Baby Jet Batch 1         400 GH/s         55600         2500 W         62/5/2014         -         -         302 Eays           MARXOWE INFO         0.1         1         440 GH/s         55600         260 W         62/5/2014         -         -         106/min/y           HashFast Baby Jet Batch 2         400 GH/s         55600         260 W         62/5/2014         -         -         106/min/y           HashFast Baby Jet Batch 2         400 GH/s         55600         40 W         62/5/2014         -         -         106/min/y           HashFast GBaby Jet Batch 2         400 GH/s         5490 W         62/5/2014         -         -         106/min/y           HashFast GBaby Jet Batch 2         400 GH/s         5493 W         62/5/2014         -         -         106/min/y           HashFast GBaby Jet Batch 2         400 GH/s         5493 W         62/5/2014         -         -	itcoin/calculator					⊽ C" 8	≠ Google				۹ 🖡	A	☆ 🗉	Ì
Difficulty increment: (?)       Speed       Price       Power       Start Date       DC       SC       MC       Break Even         0       0.01	BitcoinWisdom   Bitcoin Difficulty	Litecoin Difficulty   Bitcoin Calculator	Litecoin Calculate	or   Markets										
5       %       Conferra Ternal/ner IV       2000 GH/a       5599       1200 W       625/2014       -       -       200 GH/a         Bise List (USD/WVh)       0       01       5349       600 W       625/2014       -       -       302 days         Pool Fee:       2       %       1000 GH/a       53499       600 W       625/2014       -       -       Infinity         HashFast Baby Jet Batch 1       400 GH/a       52760       260 W       625/2014       -       -       Infinity         HashFast Baby Jet Batch 1       400 GH/a       52760       260 W       625/2014       -       -       Infinity         HashFast Baby Jet Batch 1       400 GH/a       52995       520 W       625/2014       -       -       Infinity         Hardware Price: (USD)       1200       1200 GH/a       52956       520 W       625/2014       -       -       Infinity         Hardware Price: (USD)       700       780       780 W       625/2014       -       -       Infinity         Maintain Cost (USD)       700       780       780 W       625/2014       -       -       Infinity         Maintain Cost (USD)       700       500 GH/a       5030 J	MINING SETTINGS	OVERVIEW												
S %       CoinTerra Ternal/Inter IV       2000 GH/s       5599       1200 W       6/25/2014       -       -       229 days         Deliciticity Price: (USD/AVM)       01       1       1000 GH/s       53499       660 W       6/25/2014       -       -       1000 GH/s         Pool Fee:       2       3       1       1000 GH/s       53499       660 W       6/25/2014       -       -       Infinity         HashFast Sierra Batch 2       1200 GH/s       52760       2200 W       6/25/2014       -       -       Infinity         HashFast Baby Jet Batch 1       400 GH/s       52760       2200 W       6/25/2014       -       -       Infinity         HashFast C(H/s)       1200       HashFast Starm Baby Jet Batch 1       400 GH/s       5295       320 W       6/25/2014       -       -       Infinity         HashFast C(H/s)       1200       H/s 6550       440 W       6/25/2014       -       -       Infinity         KrCMiner Jupiter       400 GH/s       54995       640 W       6/25/2014       -       -       Infinity         KrCMiner Saturn       200 GH/s       5480       350 W       6/25/2014       -       -       Infinity         Mateware Pr	Difficulty Increment: (?)	Hardware	Speed	Price	Power	Start Date	DC	SC	MC	Break Even				
Image: Second	5 9	6 CoinTerra TerraMiner IV	2000 GH/s	\$5999	1200 W	6/25/2014	-	-	-	229 days				
Image: Serie Batch 2       1200 GH/s       \$7080       780 W       625/2014       -       -       Infinity         Pool Fee:       2       %       HashFast Baby, Jet Batch 1       400 GH/s       \$5500       260 W       625/2014       -       -       Infinity         HashFast Baby, Jet Batch 2       400 GH/s       \$2500       260 W       625/2014       -       -       Infinity         BiFury Full Ki Oct       25 GH/s       6500       400 W       625/2014       -       -       Infinity         BiFury Stater Ki Oct       25 GH/s       6500       400 W       625/2014       -       -       Infinity         BiFury Stater Ki Oct       25 GH/s       52995       320 W       625/2014       -       -       Infinity         BiFury Stater Ki Oct       25 GH/s       5200       400 W       625/2014       -       -       Infinity         WIAC Platicum 1 Module       256 GH/s       5200       400 W       625/2014       -       -       Infinity         WIAC Platicum 1 Module       256 GH/s       5200       400 W       625/2014       -       -       Infinity         ButterfyLabs 600 GH/s       5903 13462 M       0.210C       ICC       ICC <t< td=""><td>Electricity Price: (USD/kWh)</td><td>CoinTerra TerraMiner II</td><td>1000 GH/s</td><td>\$3499</td><td>600 W</td><td>6/25/2014</td><td>-</td><td>-</td><td>-</td><td>302 days</td><td></td><td></td><td></td><td></td></t<>	Electricity Price: (USD/kWh)	CoinTerra TerraMiner II	1000 GH/s	\$3499	600 W	6/25/2014	-	-	-	302 days				
Pool Fee:       1       400 GH/s       \$55600       260 W       625/2014       -       -       Infinity         HashFast Baby Jet Batch 1       400 GH/s       \$52760       260 W       625/2014       -       -       Infinity         Hash Rate:       (GW)       100       100       100       100       100       100       100         Hash Rate:       (GW)       100		▶ HashFast Sierra Batch 2	1200 GH/s	\$7080	780 W	6/25/2014	-	-	-	Infinity				
Image: Start Date: (31/3)       1200         HashFast Baby Jet Batch 2       400 GH/s       52760       260 W       6252014       -       -       -       Infinity         BitFury Starter K& Oct       25 GH/s       6400 W       6252014       -       -       -       Infinity         Hash Rate: (3H/s)       [200]       1200       History Starter K& Oct       25 GH/s       6400 W       6252014       -       -       -       Infinity         KnotMmer Jupiter       400 GH/s       52995       320 W       6252014       -       -       -       Infinity         KnotMmer Jupiter       400 GH/s       52995       320 W       6252014       -       -       -       Infinity         KnotMmer Statum       200 GH/s       52903       400 W       6252014       -       -       -       Infinity         VMC Plainum f       Module       256 GH/s       5400       400 W       6252014       -       -       -       Infinity         VMC Plainum f       Module       256 GH/s       5400       400 W       6252014       -       -       -       Infinity         VMC Plainum f       Module       256 GH/s       5400       400 W       6252014 <td></td> <td>HashFast Baby Jet Batch 1</td> <td>400 GH/s</td> <td>\$5600</td> <td>260 W</td> <td>6/25/2014</td> <td>-</td> <td>-</td> <td>-</td> <td>Infinity</td> <td></td> <td></td> <td></td> <td></td>		HashFast Baby Jet Batch 1	400 GH/s	\$5600	260 W	6/25/2014	-	-	-	Infinity				
HARDWAKE INFO         HARDWAKE INFO         Hash Rate: (GH/s)         1200         Hash Rate: (GH/s)         1200         Hardware Price: (USD)         7000         Num C Platinum 1 Module       256 GH/s         51nt Date: (?)         0         Stant Date: (?)         0         0         Stant Date: (USD)         0         Naintain Cost: (USD)         0         0         10         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0         0 <td></td> <td>HashEast Baby, lat Batch 2</td> <td>400 GH/s</td> <td>\$2760</td> <td>260 W</td> <td>6/25/2014</td> <td>-</td> <td></td> <td></td> <td>Infinity</td> <td></td> <td></td> <td></td> <td></td>		HashEast Baby, lat Batch 2	400 GH/s	\$2760	260 W	6/25/2014	-			Infinity				
IXABUVAGE INFO         Hash Rate (CH4)         1200         Hash Rate (CH4)         1200         Hardware Price: (USC)         7080         Hardware Proce: (USC)         7080         Hardware Proce: (USC)         7080         Hardware Power: (Watts)         7080         Start Date: ()         100         Delivery Cost: (USD)         0         0         Start Date: ()         0 <tr< td=""><td>2 9</td><td>/o</td><td>400 GH/s</td><td>€6500</td><td>400 W</td><td>6/25/2014</td><td>-</td><td></td><td></td><td>-</td><td></td><td></td><td></td><td></td></tr<>	2 9	/o	400 GH/s	€6500	400 W	6/25/2014	-			-				
HAROWAE INFO       Hash Rate: (GH's)       Linc       Linc       Linc       Linc         Hash Rate: (GH's)       1200       H/s       52995       320 W       6/25/2014       -       -       Infinity         Hash Rate: (GH's)       1200       H/s       52995       320 W       6/25/2014       -       -       Infinity         Minitary       7000       7000       1       0       5/25/2014       -       -       Infinity         VMC Plainum 1 Module       256 GH/s       59039       1400 W       6/25/2014       -       -       Infinity         VMC Plainum 1 Module       1536 GH/s       59039       1400 W       6/25/2014       -       -       Infinity         VMC Plainum 6 Module       1536 GH/s       59039       1400 W       6/25/2014       -       -       Infinity         VMC Plainum 6 Module       1536 GH/s       59039       1400 W       6/25/2014       -       -       Infinity         VMC Plainum 6 Module       1536 GH/s       59039       1400 W       6/25/2014       -       -       -       Infinity         VMC Plainum 6 Module       1536 GH/s       59039       1400 W       6/25/2014       -       -       -       <		BitFury Starter Kit Oct	25 GH/s	€950	40 W	6/25/2014	-	-		-				
1200       KncMliner Satum       200 GH/s       \$2995       320 W       6/25/2014       -       -       Infinity         Hardware Price: (USD)       7080       YMC Platinum 1 Module       225 GH/s       \$2400       400 W       6/25/2014       -       -       Infinity         Maintain Cost: (Wats)       780       105       153 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         Maintain Cost: (USD)       10       10       6/25/2014       -       -       Infinity         Delevery Cost: (USD)       0       6/25/2014       -       -       Infinity         0       Start Date: (?)       0       10       Exception 10       0       8/27/2       0       9/27/2       0/28/25       -       10         0       Start Date: (?)       0       0       14354 M       0.2704       0/265       -       -       11.9         7.1 - 7.14 (20 days)       13462 M       0.2704       0/265       -       -       10.5         0       6/25 - 6-30 (6 days)       13462 M       0.5107       0.5005       -       -       10.5         0       6/26 - 6-30 (6 days)       11482 M       0.4591       0.4264 </td <td></td> <td>KnCMiner Jupiter</td> <td>400 GH/s</td> <td>\$4995</td> <td>640 W</td> <td>6/25/2014</td> <td>-</td> <td></td> <td>-</td> <td>Infinity</td> <td></td> <td></td> <td></td> <td></td>		KnCMiner Jupiter	400 GH/s	\$4995	640 W	6/25/2014	-		-	Infinity				
Hardware Price: (USD)       ButterflyLabs 600 GH/s       6400 GH/s       54680       350 W       6/25/2014       -       -       Infinity         VMC Platinum 1 Module       256 GH/s       52400       400 W       6/25/2014       -       -       Infinity         VMC Platinum 1 Module       256 GH/s       52400       400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       Infinity         VMC Platinum 6 Module       1536 GH/s       \$9039       1400 W       6/25/2014       -       -       101111         Delivery Cost: (USD)       0       10       -       -       - <td< td=""><td>Hash Rate: (GH/s)</td><td>KnCMiner Saturn</td><td>200 GH/s</td><td>\$2995</td><td>320 W</td><td>6/25/2014</td><td>-</td><td>-</td><td>-</td><td>Infinity</td><td></td><td></td><td></td><td></td></td<>	Hash Rate: (GH/s)	KnCMiner Saturn	200 GH/s	\$2995	320 W	6/25/2014	-	-	-	Infinity				
Total       Total       Total       Total       Total       Total       Total         Normalization       1	1200	ButterflyLabs 600 GH/s	600 GH/s	\$4680	350 W	6/25/2014	-	-	-	Infinity				
Hardware       Power: (Watts)       1 <th1< th=""> <th1< th="">       1       1</th1<></th1<>	Hardware Price: (USD)	VMC Platinum 1 Module	256 GH/s	\$2400	400 W	6/25/2014	-	-	-	Infinity				
TRASHFAST SIERRA BATCH 2       DISPLAY CURRENCY:       O BTC       LTC       USD       EUR       O(NY)         Start Date:       (?)       I	7080	VMC Platinum 6 Module	1536 GH/s	\$9039	1400 W	6/25/2014	-	-	-	Infinity				
Start Date: (?)       Display Concentry: or pic       Clic UC	Hardware Power: (Watts)													
Start Date: (?)       Group By: Difficulty Day       Week       Month         Delivery Cost: (USD)       0       Date       Difficulty       Revenue       Profit       Return         2014	780	HASHEAST SIEDDA BATCH 2					O PTC	O LTC						
Date         Difficulty         Revenue         Profit         Return           Delivery Cost: (USD)         0         -12.16	Start Date: (?)				DISPLAT									
Delivery Cost: (USD)         Date         Difficulty         Revenue         Profit         Return           0.00         0.00         0.00         0.00         0.00         0.00         0.00         0         0.00         0         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0.00         0	300*					Group By: @	Difficult	y   Di	ay 💿 We	ek 💿 Month				
2014       -12.16         6-25 - 6-30 (6 days)       13462 M       0.2704       0.265       -11.9         0			Diffic	culty	Reve	enue	Pr	ofit		Return				
Setup Cost: (USD)       6-25 - 6-30 (6 days)       13462 M       0.2704       0.265       -11.9         Naintain Cost: (USD)       7.1 - 7.14 (20 days)       14135 M       0.5385       0.5277       -11.37         7.15 - 7.27 (33 days)       14842 M       0.5107       0.5005       -10.87         7.28 - 8-10 (47 days)       15584 M       0.4843       0.4746       -10.4         8-11 - 8-24 (61 days)       16363 M       0.4591       0.4499       -9.947         8-25 - 9-6 (74 days)       17182 M       0.4351       0.4264       -9.521         9-7 - 9-20 (88 days)       18041 M       0.4122       0.404       -9.117         9-21 - 10-4 (102 days)       18943 M       0.3905       0.3827       -8.734         10-5 - 10-17 (115 days)       19890 M       0.3697       0.3623       -8.372         10-18 - 10-31 (129 days)       20884 M       0.35       0.343       -8.029         11-1 - 11-14 (143 days)       21929 M       0.3312       0.3246       -7.704         11-15 - 11-27 (115 days)       23025 M       0.3133       0.307       -7.397										-12.16				
Imain Cost: (USD/Month)       Imain Cost: (USD/Month) <td></td> <td>6-25 – 6-30 (6 days)</td> <td>1346</td> <td>2 M</td> <td>0.2</td> <td>704</td> <td>0.</td> <td>265</td> <td></td> <td>-11.9</td> <td></td> <td></td> <td></td> <td></td>		6-25 – 6-30 (6 days)	1346	2 M	0.2	704	0.	265		-11.9				
Maintain Cost: (USD/Month)       7-16 - 7-27 (35 days)       14642 M       0.5107       0.5005       -10.67         Maintain Cost: (USD/Month)       7-28 - 8-10 (47 days)       15584 M       0.4843       0.4746       -10.4         8-11 - 8-24 (61 days)       16363 M       0.4591       0.4999       -9.947         8-25 - 9-6 (74 days)       17182 M       0.4351       0.4264       -9.521         9-7 - 9-20 (88 days)       18041 M       0.4122       0.404       -9.117         9-7 - 9-20 (88 days)       18943 M       0.3905       0.3827       -8.734         10-5 - 10-17 (115 days)       19890 M       0.3697       0.3623       -8.372         10-18 - 10-31 (129 days)       20884 M       0.35       0.343       -8.029         11-1 - 11-14 (143 days)       21929 M       0.3312       0.3246       -7.704         11-15 - 11-27 (156 days)       23025 M       0.3133       0.307       -7.397		<b>7-1 – 7-14</b> (20 days)	1413	5 M	0.5	385	0.6	277		-11.37				
Image: Constraints       8-11 - 8-24 (61 days)       16363 M       0.4459       0.4499       -9.947         8-25 - 9-6 (74 days)       16363 M       0.4591       0.4499       -9.947         8-25 - 9-6 (74 days)       17182 M       0.4351       0.4264       -9.521         9-7 - 9-20 (88 days)       18041 M       0.4122       0.404       -9.117         9-7 - 9-20 (88 days)       18943 M       0.3905       0.3827       -8.734         10-5 - 10-17 (115 days)       19890 M       0.3697       0.3623       -8.372         10-18 - 10-31 (129 days)       20884 M       0.35       0.343       -8.029         11-1 - 11-14 (143 days)       21929 M       0.3312       0.3246       -7.704         11-15 - 11-27 (156 days)       23025 M       0.3133       0.307       -7.397		7-15 – 7-27 (33 days)	1484	2 M	0.5	107	0.5	5005		-10.87				
CONSTANTS         8-25 - 9-6 (74 days)         17182 M         0.4351         0.4264         -9.521           BTC/USD:         9-7 - 9-20 (88 days)         18041 M         0.4122         0.404         -9.117           582         10-5 - 10-17 (115 days)         18943 M         0.3905         0.3827         -8.734           10-5 - 10-17 (115 days)         19890 M         0.3697         0.3623         -8.372           10-18 - 10-31 (129 days)         20884 M         0.35         0.343         -8.029           11-1 - 11-14 (143 days)         21929 M         0.3132         0.307         -7.397	Maintain Cost: (USD/Month)	7-28 – 8-10 (47 days)	1558	4 M	0.4	843	0.4	746		-10.4				
CONSTANTS         9-7 - 9-20 (88 days)         18041 M         0.4122         0.404         -9.117           BTC/USD:         9-21 - 10-4 (102 days)         18943 M         0.3905         0.3827         -8.734           10-5 - 10-17 (115 days)         19890 M         0.3697         0.3623         -8.372           10-5 - 10-17 (115 days)         19890 M         0.355         0.343         -8.029           11-1 - 11-14 (143 days)         21929 M         0.3312         0.3246         -7.704           11-15 - 11-27 (156 days)         23025 M         0.3133         0.307         -7.397	0	8-11 – 8-24 (61 days)	1636	3 M	0.4	591	0.4	499		-9.947				
BTC/USD:         9-21 - 10-4 (102 days)         18943 M         0.3905         0.3827         -8.734           LTC/USD:         10-5 - 10-17 (115 days)         19890 M         0.3697         0.3623         -8.372           9.55         10-18 - 10-31 (129 days)         20884 M         0.35         0.343         -8.029           11-1 - 11-14 (143 days)         21929 M         0.3312         0.3246         -7.704           11-15 - 11-27 (156 days)         23025 M         0.3133         0.307         -7.397		8-25 - 9-6 (74 days)	1718	2 M	0.4	351	0.4	264		-9.521				
582         10-5 - 10-17 (115 days)         19890 M         0.3697         0.3623         -8.372           LTC/USD:         10-18 - 10-31 (129 days)         20884 M         0.35         0.343         -8.029           9.55         11-1 - 11-14 (143 days)         21929 M         0.3312         0.3246         -7.704           11-15 - 11-27 (156 days)         23025 M         0.3133         0.307         -7.397	CONSTANTS	<b>9-7 – 9-20</b> (88 days)	1804	1 M	0.4	122	0.	404		-9.117				
LTC/USD: 9.55 10-18 - 10-31 (129 days) 20884 M 0.35 0.343 -8.029 11-1 - 11-14 (143 days) 21929 M 0.3312 0.3246 -7.704 11-15 - 11-27 (156 days) 23025 M 0.3133 0.307 -7.397	BTC/USD:	9-21 – 10-4 (102 days)	1894	3 M	0.3	905	0.3	827		-8.734				
9.55 11-1 - 11-14 (143 days) 21929 M 0.3312 0.3246 -7.704 11-15 - 11-27 (156 days) 23025 M 0.3133 0.307 -7.397	582	<b>10-5 – 10-17</b> (115 days)	1989	0 M	0.3	697	0.3	8623		-8.372				
955 11-15 - 11-27 (156 days) 23025 M 0.3133 0.307 -7.397	LTC/USD:	<b>10-18 – 10-31</b> (129 days)	2088	4 M	0.	35	0.	343		-8.029				
11-15 – 11-27 (156 days) 23025 M 0.3133 0.307 -7.397		<b>11-1 – 11-14</b> (143 days)	2192	9 M	0.3	312	0.3	3246		-7.704				
	BTC/EUR:	11-15 – 11-27 (156 days)	2302	5 M	0.3	133	0.	307		-7.397				

NanoCAD Lab

#### puneet@ee.ucla.edu

24176 M

0 2962

0 2903

-7 107

11-28 - 12-11 (170 days)



# **Bitcoin Mining Pools**

- Bitcoin mining is a very risky venture
  - As soon as one miner solves the puzzle, all others must restart on the next block
- Typically done in pools
  - All miners in pool share rewards for a successful mine
  - Miners who contribute more 'partial' solutions get greater share of reward
  - Several different miners with different protocols for joining, sharing, etc.



# References

- Good Explanation of Bitcoin: <u>http://www.michaelnielsen.org/ddi/how-the-</u> <u>bitcoin-protocol-actually-works/</u>
- Tutorial videos on Khan Academy: https://www.khanacademy.org/economicsfinance-domain/core-finance/money-andbanking/bitcoin/v/bitcoin-what-is-it
- Hardware for Mining: http://www.tomshardware.com/reviews/bitcoinmining-make-money,3514-3.html

