Use of FPGAs in Cryptocurrencies

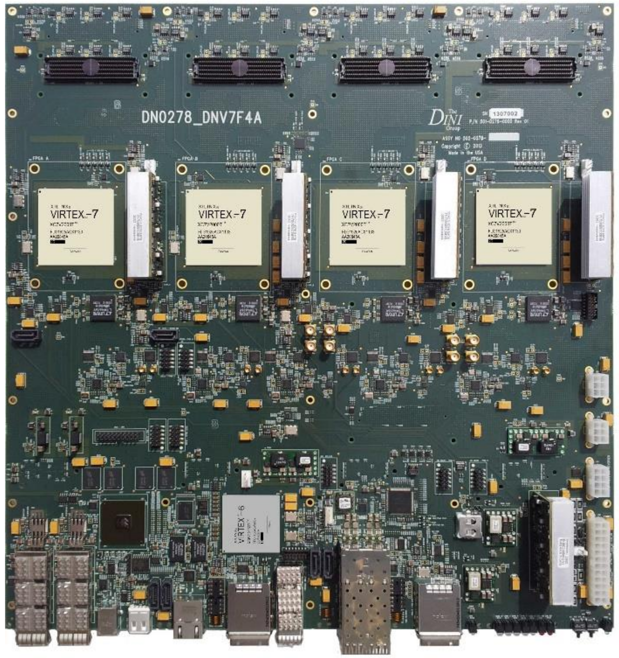
FPGA World 2014
September 9, 2014

Mike Dini

DINI Group

!!!!!! Disclosures !!!!!!

- Mike Dini
  - President of DINI Group
- Don’t own any of this stuff.
- Won’t knowingly sell our products into this market.
- Don’t take financial advice from me!
  - Maybe do exactly opposite of what I say …
- Value of Bitcoin as of 1pm (Sweden time): $466
- (off topic sales pitch)
  - We make BIG FPGA boards:



Overview

- What is a ‘cryptocurrency’?
  - What are they? How do they work?
  - Overview of the various different cryptocurrencies
  - Where are they used?
  - Mining
  - The problems

- How did FPGAs get involved?

What is a cryptocurrency (bitcoin)?

- Decentralized digital currency
  - Not backed by a **fiat** currency. No $ or €. What is money?
  - In the ‘cloud’.
  - public transactions, no central authorities, cryptographically secured transactions, peer-to-peer transaction propagation
  - Loose organization controlling
  - Arguably anonymous
- Started with a paper by Satoshi Nakamoto
  - We don’t know who he is but he is not this guy →
    - NEWS! Email hacked …
  - But he appears to have about 1 million BTC
    - ~$500M if you could convert it to cash
      - Which you can’t …..
- Open Source → Alternate implementations (altcoins)
  - Let the party BEGIN!!!

The various Cryptocurrencies

- Bitcoin
  - SHA256. FFs and POWER!
    - 10 minutes?
- LiteCoin
  - Make mining harder to do via ASIC by making it memory intensive
    - Scrypt: GPUs?
    - Faster transactions
- Steep dropoff to **altcoins**:
  - NXT
  - Ripple
  - Peercoin
  - Darkcoin
  - Dogecoin
    - After the dude’s dog?

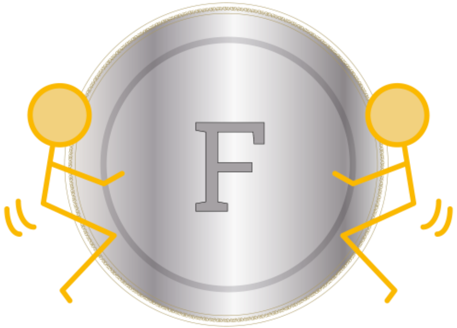
Star Power behind bitcoin

- Like it:
    - Rapper 50 Cent
    - The Winklevoss Twins (Facebook fame) have 108,000 BTC and want to start a ETF
    - Good many ignorant venture capitalists
    - Ben Bernake “may hold long-term promise”
    - Marc Andreessen (Netscape founder) – “Bitcoin offers a sweeping vista of opportunity”
    - David Woo (BofA/ML) “As a medium of exchange, Bitcoin has clear potential for growth, in our view.”
    - David Marcus (Pres of PayPal) “I really like Bitcoin. I own bitcoins.”
    - Sir Richard Branson will sell you a ticket to space on Virgin Galactic
    - Al Gore – “I’m a big fan of Bitcoin”
- Hate it:
    - Jamie Dimon (CEO JPM) – “Bitcoin is a terrible store of value.”
    - Jim Cramer (Mad Money) said that without a central bank Bitcoin is not a currency and “the Treasury should have shut down Bitcoin”
    - The Washington Post: “Bitcoin is ludicrous”
    - The New York Times: “How can bitcoin be anything but a passing fad?”
    - Paul Krugman (Nobel winning Keynesian Economist) – “Bitcoin is Evil”

Altcoins (100’s of these) ….

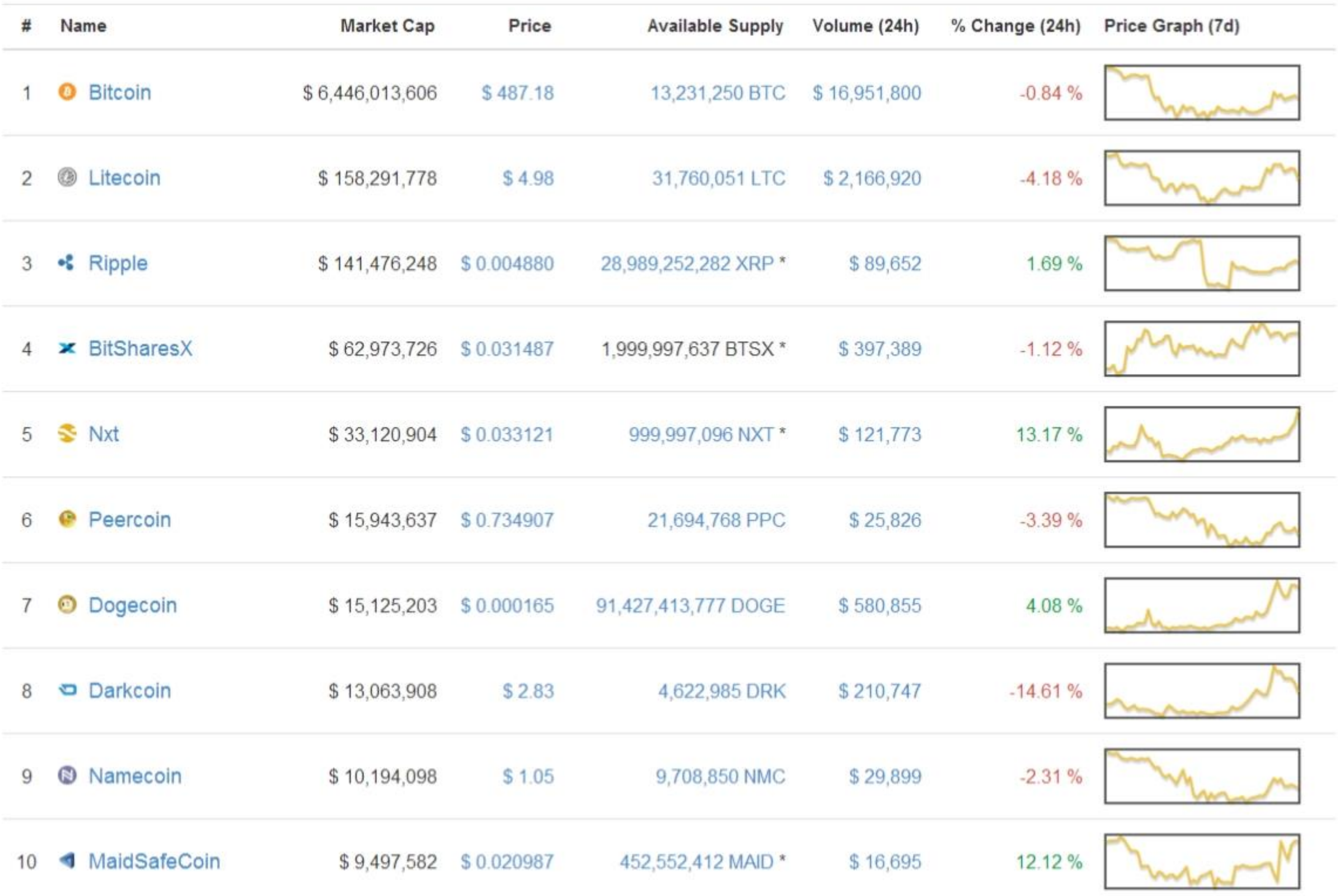
- Altcoins: Different mining strategy. Different transaction protocols.

- Dogs (Dogecoin), ~~hip-hop (Coinye)~~, Sexcoin (also XXXcoin, Titcoin, Wankcoin), Yolocoin, Lebowskis, Potcoin, Kimcoin, Coindashian (Koindashian?), Catcoin (of course …), Murraycoin, ***kCoin (2 competing versions!)



wow much coin how money so crypto plz mine v rich very currency
WOW

COINYE



#	Name	Market Cap	Price	Available Supply	Volume (24h)	% Change (24h)	Price Graph (7d)
1	Bitcoin	$ 6,446,013,606	$ 487.18	13,231,250 BTC	$ 16,951,800	-0.84 %	
2	Litecoin	$ 158,291,778	$ 4.98	31,760,051 LTC	$ 2,166,920	-4.18 %	
3	Ripple	$ 141,476,248	$ 0.004880	28,989,252,282 XRP *	$ 89,652	1.69 %	
4	BitSharesX	$ 62,973,726	$ 0.031487	1,999,997,637 BTSX *	$ 397,389	-1.12 %	
5	Nxt	$ 33,120,904	$ 0.033121	999,997,096 NXT *	$ 121,773	13.17 %	
6	Peercoin	$ 15,943,637	$ 0.734907	21,694,768 PPC	$ 25,826	-3.39 %	
7	Dogecoin	$ 15,125,203	$ 0.000165	91,427,413,777 DOGE	$ 580,855	4.08 %	
8	Darkcoin	$ 13,063,908	$ 2.83	4,622,985 DRK	$ 210,747	-14.61 %	
9	Namecoin	$ 10,194,098	$ 1.05	9,708,850 NMC	$ 29,899	-2.31 %	
10	MaidSafeCoin	$ 9,497,582	$ 0.020987	452,552,412 MAID *	$ 16,695	12.12 %	

474 currencies listed, but number 430 had market cap of $27

Basics: Create the coins

- Problem created
  - Transactions are published to the Bitcoin peer to peer network
- Miners (computers) compete to solve SHA256 (or other) problem on average every 10 minutes
  - Created an arms race …
- First solution (winner) publishes a summary of recent transactions in the blockchain
- Miners are rewarded with new coins for having published a valid block
  - Blocks are linked to previous blocks, creating a block chain
  - The value of every account is evident on the blockchain
  - Everyone is expected to know the whole blockchain

Where are they used?

- Online purchases
- Tips and donations
- Micro-payments
- Embarrassing transactions
  - A place to hide money
  - Gambling
  - Ransom
  - Black-market transactions
    - Silk Road

- Escape currencies that are in trouble
  - Cyprus
- International transactions and financing
- Buying foreign goods
- Paying foreign employees

Where are they used?

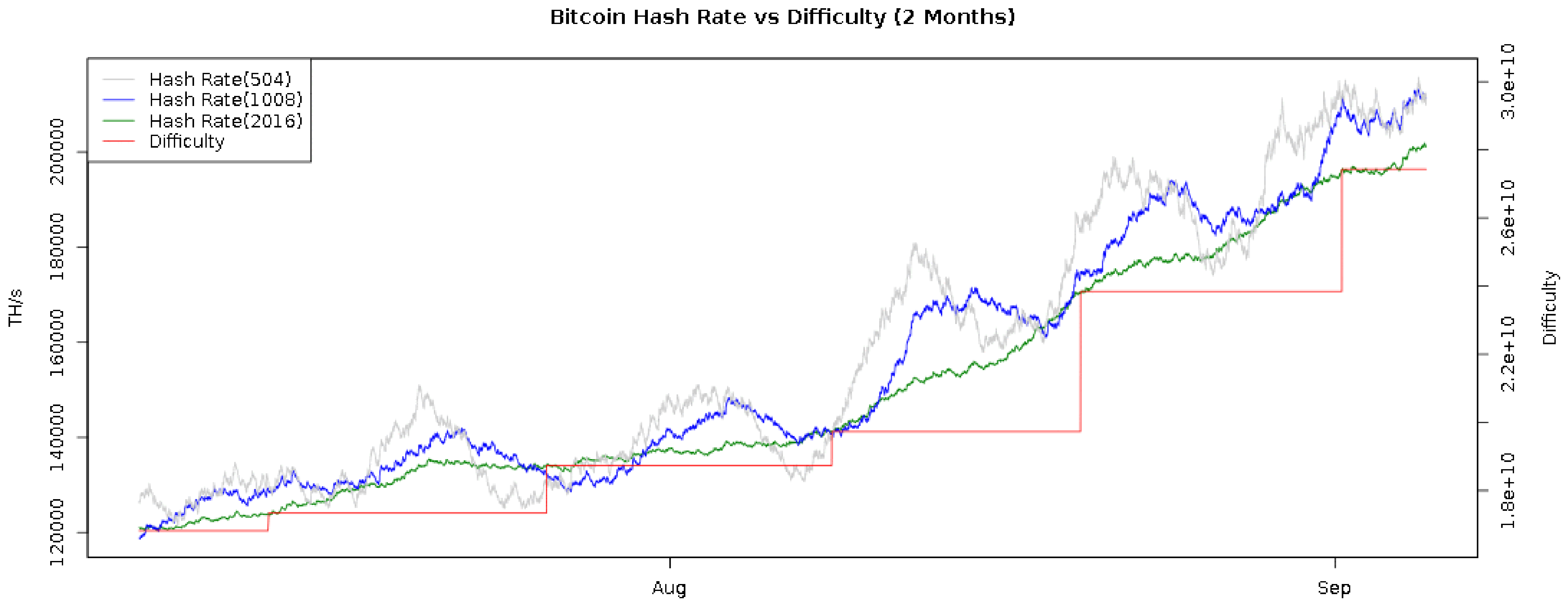
wow much coin how money so crypto plz mine v rich very currency
WOW

From Burning Man Festival …

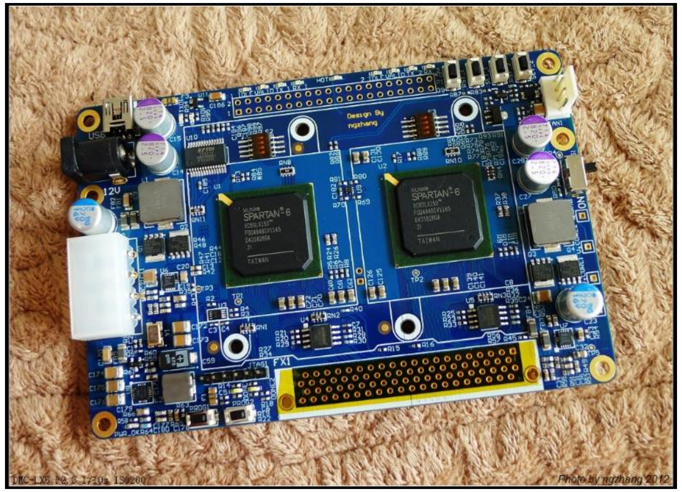
Mining – This is where FPGAs get involved

- Bitcoin mining started on CPUs
  - GPUs got in the mix
  - Followed by FPGAs
  - ASICs now are required.
  - Litecoin is mainly GPUs
    - Rumors of a pending ASIC

- SHA256 is a ‘crypto’. This means solving the problem means a high FF toggle.
  - Power!

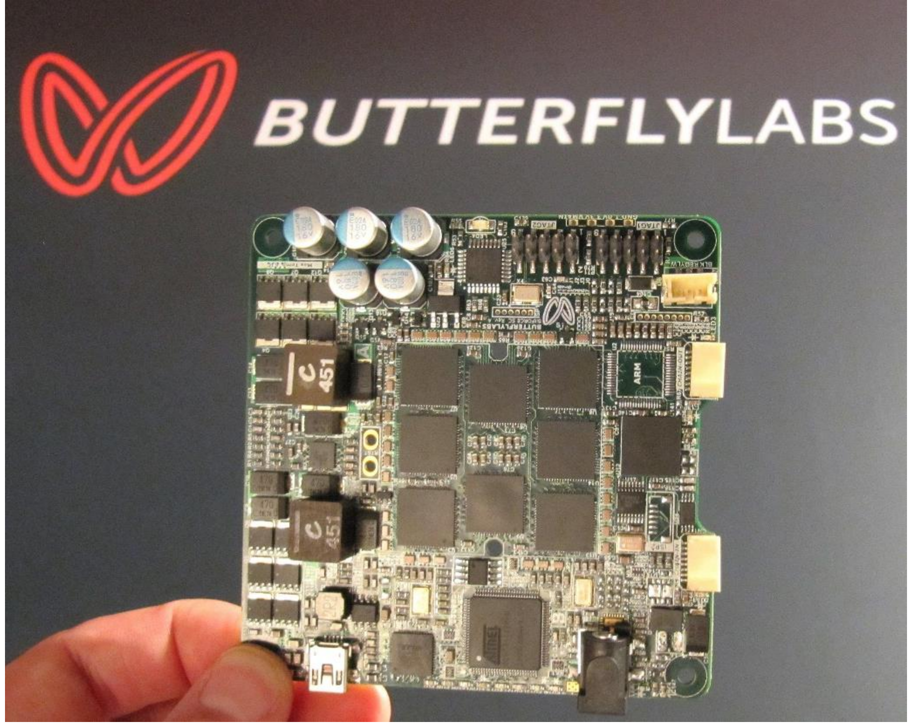

Bitcoin Hash Rate vs Difficulty (2 Months)
Hash Rate(504)
Hash Rate(1008)
Hash Rate(2016)
Difficulty
TH/s
120000
140000
160000
180000
200000
Aug
Sep
Difficulty
1.8e+10
2.2e+10
2.6e+10
3.0e+10

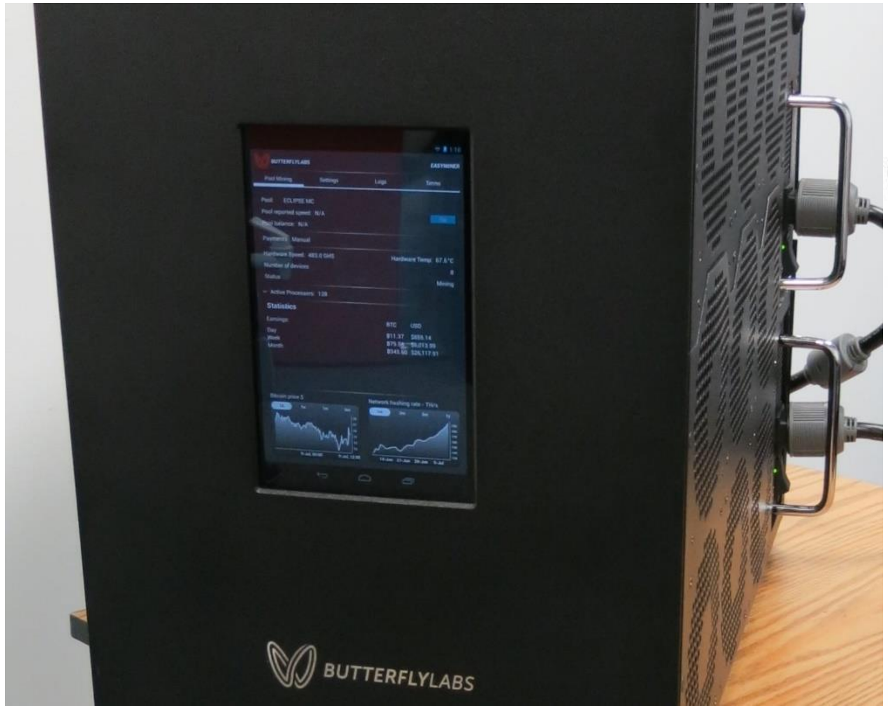
Raspberry Pi



Heat and power are an issue …

PRIORITY MAIL
msi


BUTTERFLYLABS

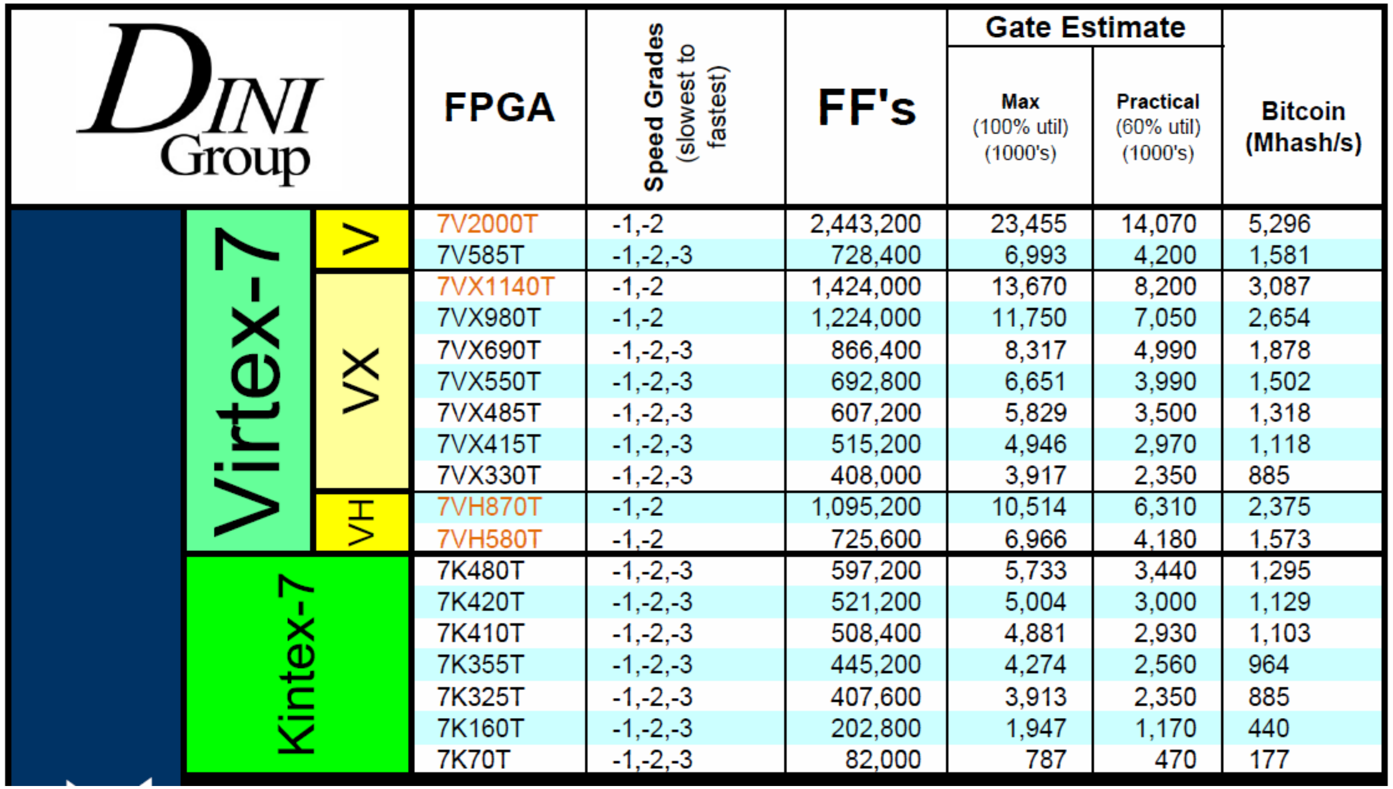

BUTTERFLYLABS

State of the art ASIC (changes hourly)

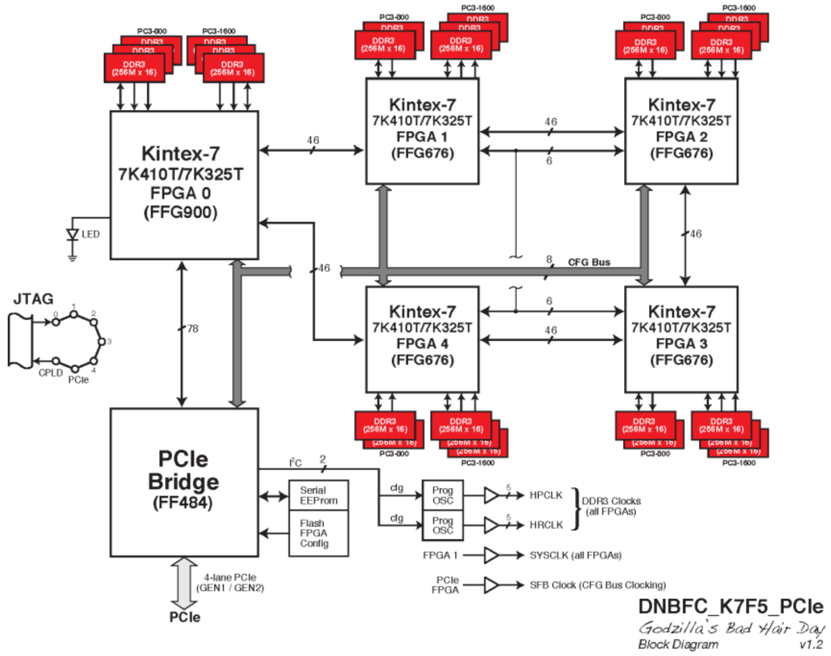
- CoinTerra Miner IV
  - 1.6 TH/s (2?), $6000, 1200W
  - $6000/(2,000 Ghash/s) = $3
- Yields .88 BTC/month
  - At present difficulty and BTC value
  - .88*$500=$440
  - Need to add in cost of electricity

State of the art Bitcoin mining: FPGA

- Use DINI Group DNK7_F5PCIe as example



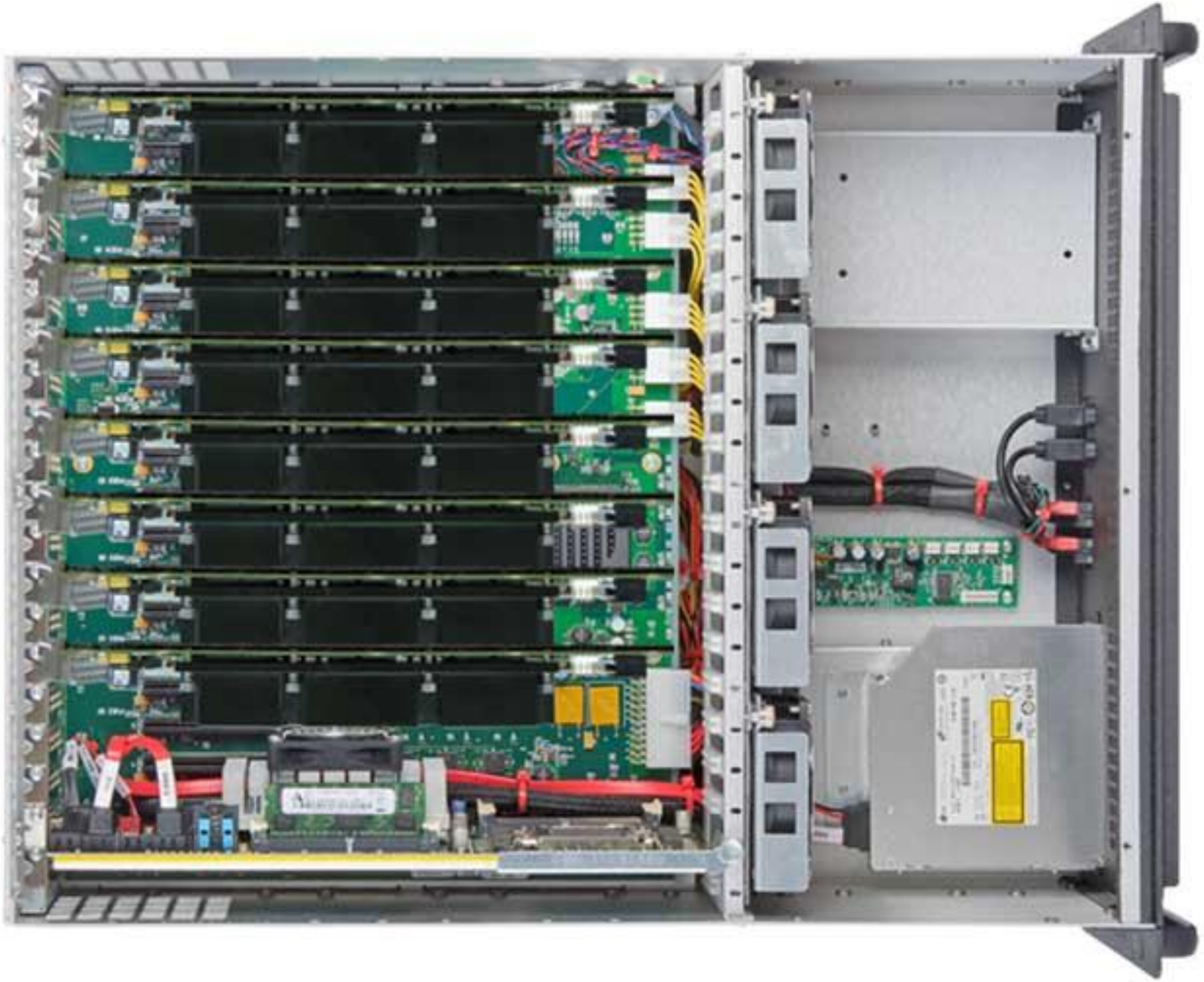
DINI Group		FPGA	Speed Grades (slowest to fastest)	FF's	Gate Estimate		Bitcoin (Mhash/s)
					Max (100% util) (1000's)	Practical (60% util) (1000's)	
Virtex-7	V	7V2000T	-1,-2	2,443,200	23,455	14,070	5,296
		7V585T	-1,-2,-3	728,400	6,993	4,200	1,581
	VX	7VX1140T	-1,-2	1,424,000	13,670	8,200	3,087
		7VX980T	-1,-2	1,224,000	11,750	7,050	2,654
		7VX690T	-1,-2,-3	866,400	8,317	4,990	1,878
		7VX550T	-1,-2,-3	692,800	6,651	3,990	1,502
		7VX485T	-1,-2,-3	607,200	5,829	3,500	1,318
		7VX415T	-1,-2,-3	515,200	4,946	2,970	1,118
		7VX330T	-1,-2,-3	408,000	3,917	2,350	885
	VH	7VH870T	-1,-2	1,095,200	10,514	6,310	2,375
		7VH580T	-1,-2	725,600	6,966	4,180	1,573
Kintex-7		7K480T	-1,-2,-3	597,200	5,733	3,440	1,295
		7K420T	-1,-2,-3	521,200	5,004	3,000	1,129
		7K410T	-1,-2,-3	508,400	4,881	2,930	1,103
		7K355T	-1,-2,-3	445,200	4,274	2,560	964
		7K325T	-1,-2,-3	407,600	3,913	2,350	885
		7K160T	-1,-2,-3	202,800	1,947	1,170	440
		7K70T	-1,-2,-3	82,000	787	470	177



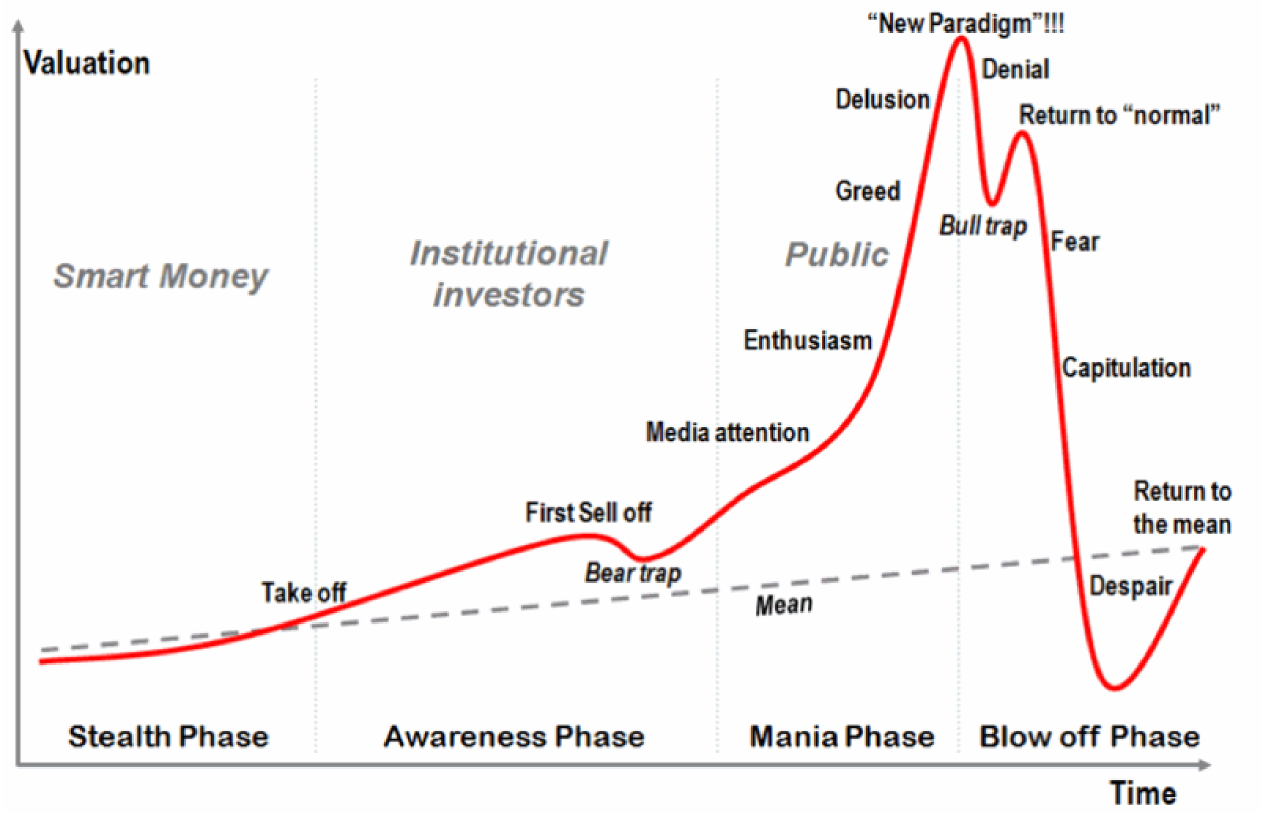
5.5 Ghash/sec. $15k

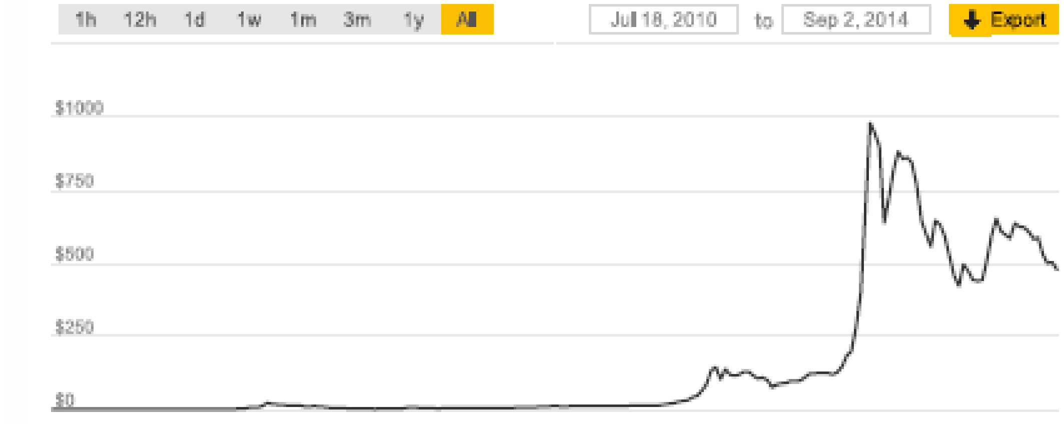
Cluster?

- 8 boards, 44 Ghash/s, $125k
  - 400W
  - $2,840/Ghash/s



Bubble?





From WikiMedia Commons

Advantages/Problems?

- Non reversible transaction
- Very volatile
- Not yet achieved critical mass
- Cool way to avoid taxes and other fees
- Blockchain bloat.
- Malleability

FPGAs in the mix?

- Sadly, no.
- What would have to happen for FPGAs to get into the mix?