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

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?

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!
Heat and power are an issue ...
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

<table>
<thead>
<tr>
<th>FPGA</th>
<th>Speed Grades (slowest to fastest)</th>
<th>FF's</th>
<th>Gate Estimate</th>
<th>Bitcoin (Mhash/s)</th>
</tr>
</thead>
<tbody>
<tr>
<td>7V2000T</td>
<td>-1, -2</td>
<td>2,443,200</td>
<td>23,455</td>
<td>14,070</td>
</tr>
<tr>
<td>7V585T</td>
<td>-1, -2</td>
<td>728,400</td>
<td>6,993</td>
<td>4,200</td>
</tr>
<tr>
<td>7VX1140T</td>
<td>-1, -2</td>
<td>1,424,000</td>
<td>13,670</td>
<td>8,200</td>
</tr>
<tr>
<td>7VX980T</td>
<td>-1, -2</td>
<td>1,224,000</td>
<td>11,750</td>
<td>7,050</td>
</tr>
<tr>
<td>7VX690T</td>
<td>-1, -2</td>
<td>866,400</td>
<td>8,317</td>
<td>4,990</td>
</tr>
<tr>
<td>7VX550T</td>
<td>-1, -2</td>
<td>692,800</td>
<td>6,651</td>
<td>3,990</td>
</tr>
<tr>
<td>7VX485T</td>
<td>-1, -2</td>
<td>607,200</td>
<td>5,829</td>
<td>3,500</td>
</tr>
<tr>
<td>7VX415T</td>
<td>-1, -2</td>
<td>515,200</td>
<td>4,946</td>
<td>2,970</td>
</tr>
<tr>
<td>7VX330T</td>
<td>-1, -2</td>
<td>408,000</td>
<td>3,917</td>
<td>2,350</td>
</tr>
<tr>
<td>7VH870T</td>
<td>-1, -2</td>
<td>1,095,200</td>
<td>10,514</td>
<td>6,310</td>
</tr>
<tr>
<td>7VH580T</td>
<td>-1, -2</td>
<td>725,600</td>
<td>6,966</td>
<td>4,180</td>
</tr>
<tr>
<td>7K480T</td>
<td>-1, -2</td>
<td>597,200</td>
<td>5,733</td>
<td>3,440</td>
</tr>
<tr>
<td>7K420T</td>
<td>-1, -2</td>
<td>521,200</td>
<td>5,004</td>
<td>3,000</td>
</tr>
<tr>
<td>7K410T</td>
<td>-1, -2</td>
<td>508,400</td>
<td>4,881</td>
<td>2,930</td>
</tr>
<tr>
<td>7K355T</td>
<td>-1, -2</td>
<td>445,200</td>
<td>4,274</td>
<td>2,560</td>
</tr>
<tr>
<td>7K325T</td>
<td>-1, -2</td>
<td>407,600</td>
<td>3,913</td>
<td>2,350</td>
</tr>
<tr>
<td>7K160T</td>
<td>-1, -2</td>
<td>202,800</td>
<td>1,947</td>
<td>1,170</td>
</tr>
<tr>
<td>7K70T</td>
<td>-1, -2</td>
<td>82,000</td>
<td>787</td>
<td>479</td>
</tr>
</tbody>
</table>

5.5 Ghash/sec. $15k
Cluster?

• 8 boards, 44 Ghash/s, $125k
  • 400W
  • $2,840/Ghash/s
Bubble?

From [WikiMedia Commons](https://commons.wikimedia.org/wiki/File:Bubble_chart.svg)
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?