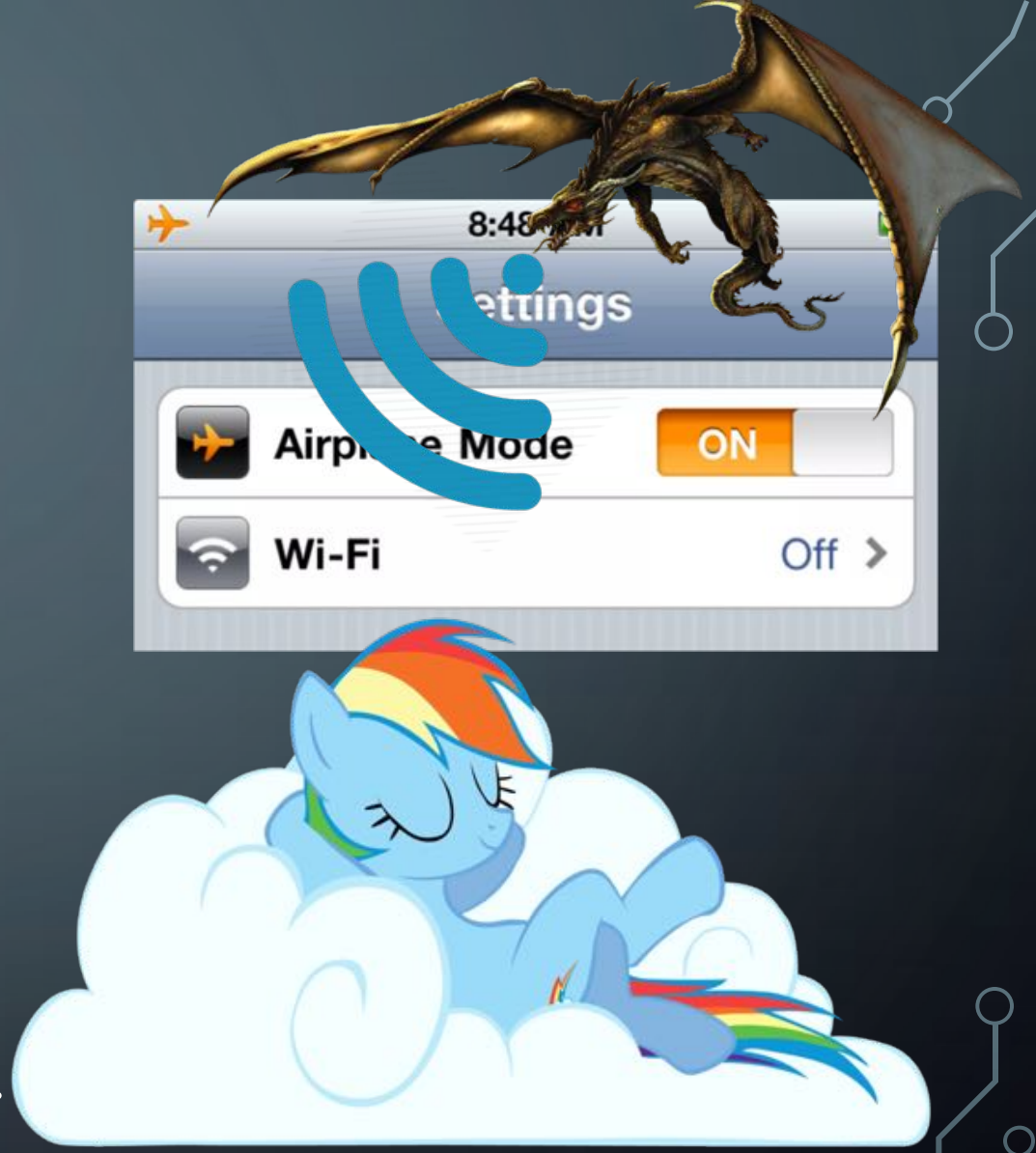
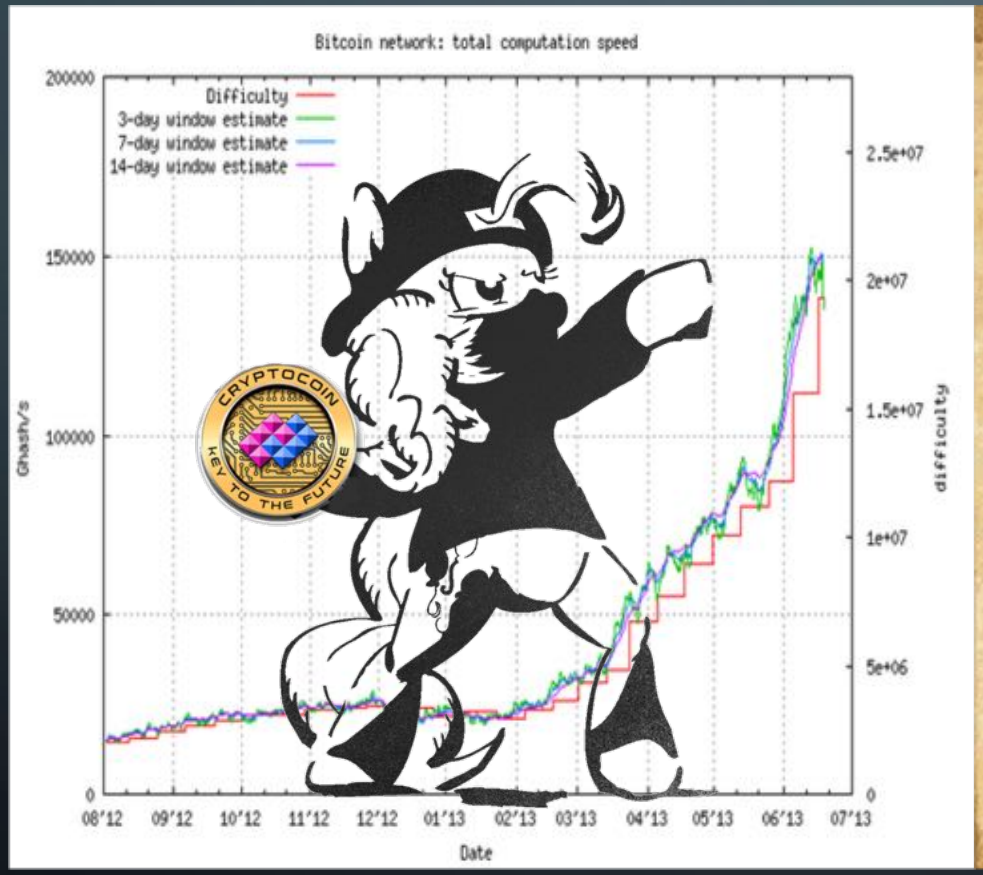
A BLOCKCHAIN QUEST

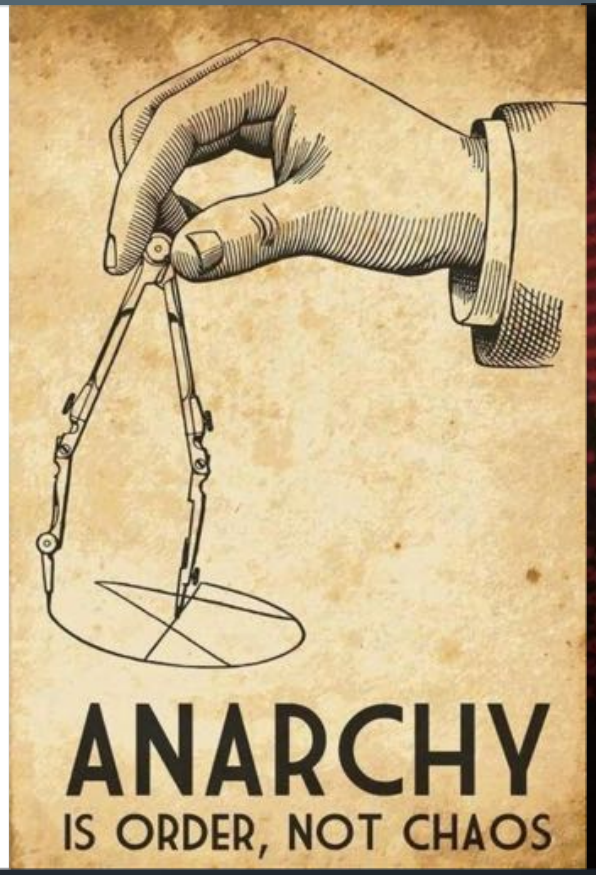
INTRODUCTIONS

- Hacker Fantastic, Co-Founder Hacker House
- Security training and professional services
- Why listen?
- Talk contains a live demo, participation optional.



Ⓐ ANARCHY vs WOLF $ STREET





THIS ISN'T JUST ABOUT MONEY…

- Blockchains are a new computer paradigm
- De-centralized Trust
- Peer-2-Peer
- Privacy orientated
- Secured with Cryptography
- Censorship Resistant
- Open World Order vs New World Order
- Machine-Aided Consensus
- Increased Connectivity
- Decreased Overheads
- **Problem Solving** Potential

REVOLUTION

CRYPTO CYBER CRIME WAVE

Hackers stole $400 million from cryptocurrency exchange Coincheck

500 Million NEM tokens were stolen

Technology Intelligence

Coincheck hackers trying to move stolen cryptocurrency after major Japanese heist

share

Hackers steal $64 mil… crypto… N…

RAMPANT FRAUD, US-SEC & *MONEY LAUNDERING*

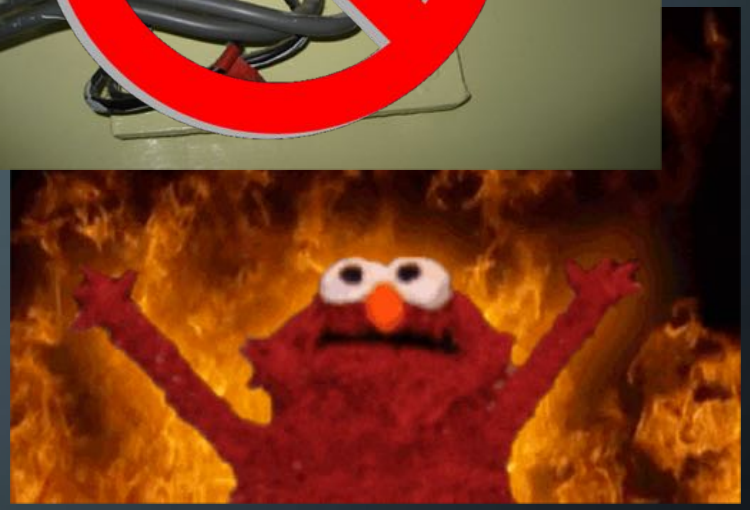
- ICO's are dangerously misleading, often solving no real problem
- Regulation tries to curb & control, questions legitimacy
- Media hysteria, lack of understanding, misinformed old television & young facebook generations. #FAKEnews, Cambridge Analytica, feeds of "Get Rich, Bitcoin" scams. Social capital.
- Fools & their money are easily parted

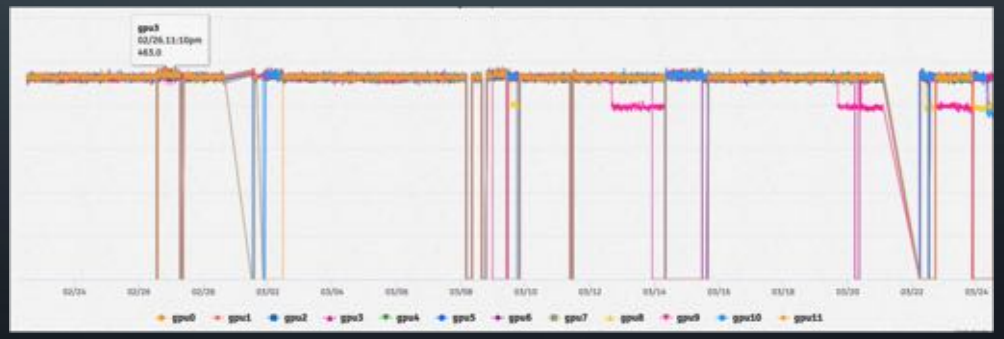
YOU ENTER THE TAVERN…

- Quest through lifecycles of “Mining”
- Proof-of-Work Puzzle Consensus Acceleration
- Digital Design, Modelling & Simulations
- Outputs

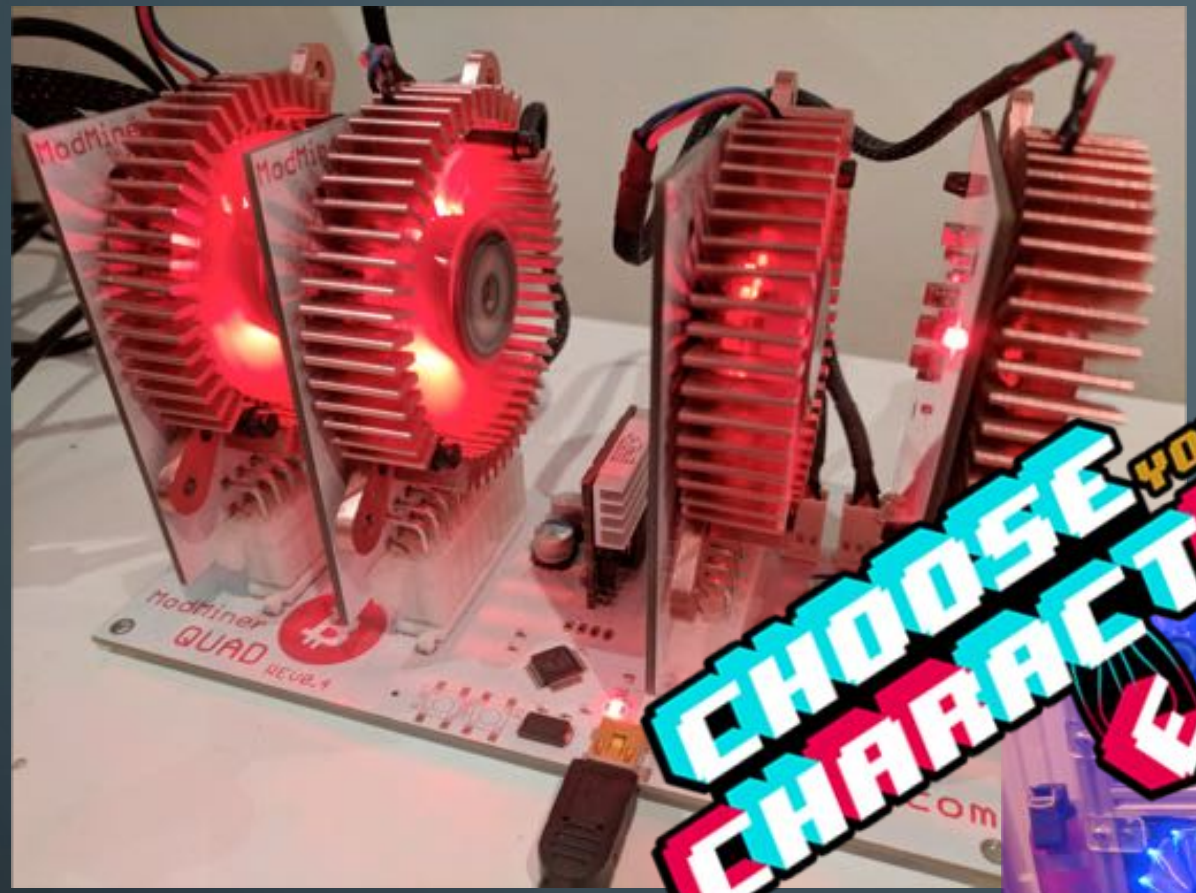
EQUIP YOUR PARTY WISELY!

- *Electrical engineering primer is recommended*, health & safety 101, electricity is serious business +1
- Know Ohms law, Watts, Amps, kWh, IC's, Maker etc.
- **1-10-100 mA** rule, ***please avoid death!***
- Avoid fires by using ***proper rated wiring***, for **ALL PARTS OF INSTALLATION**! Keep to 10A max per socket, don't overload the ring!






ROUND
ONE



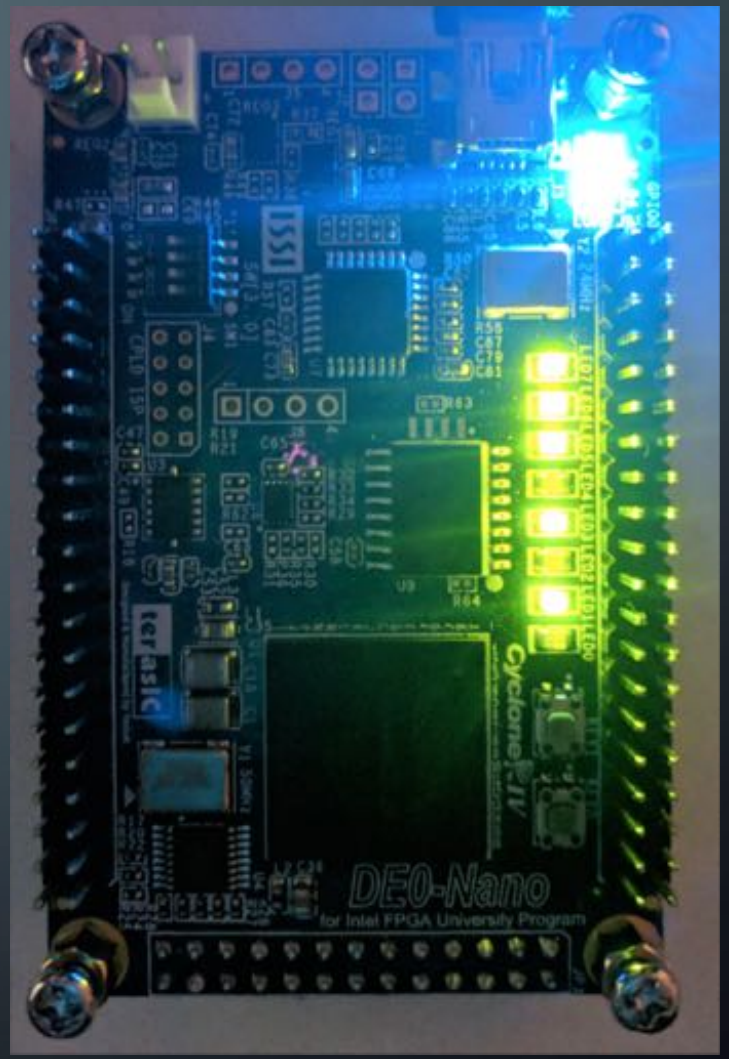
... FPGA

GPU ...

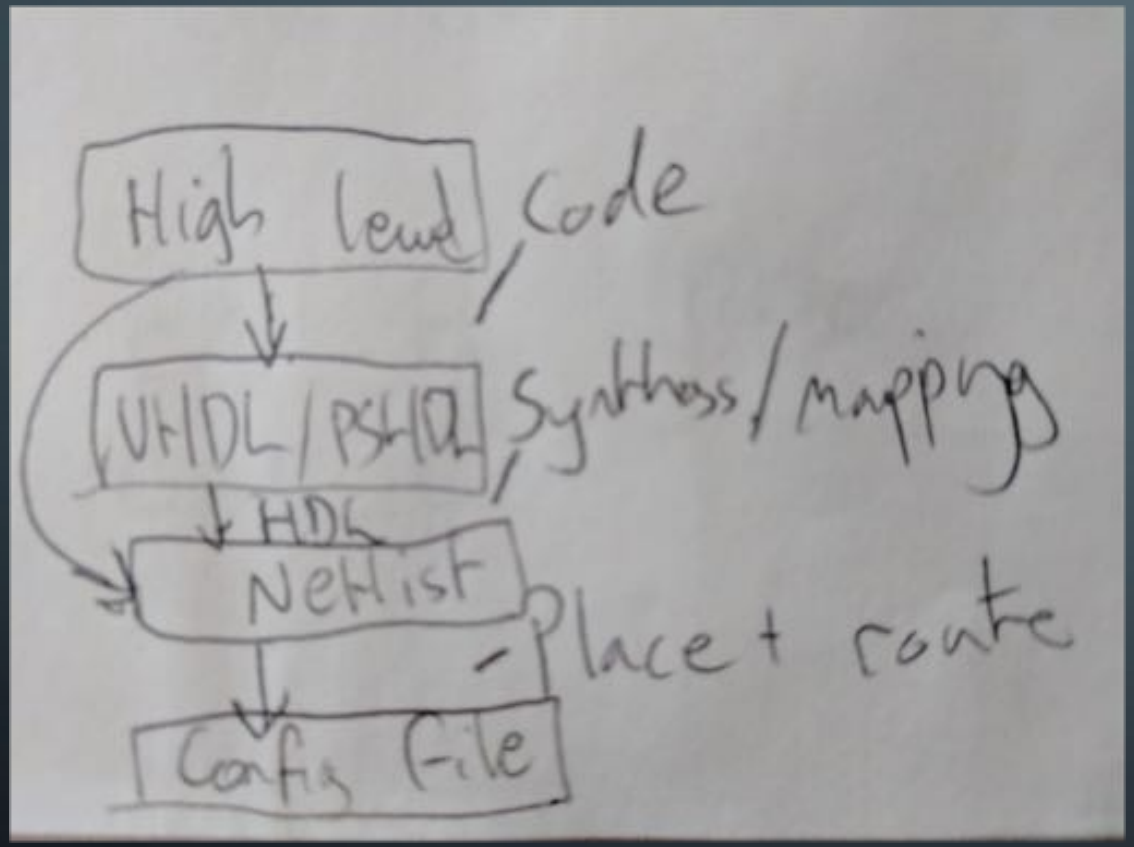
DEVELOPMENT BOARD

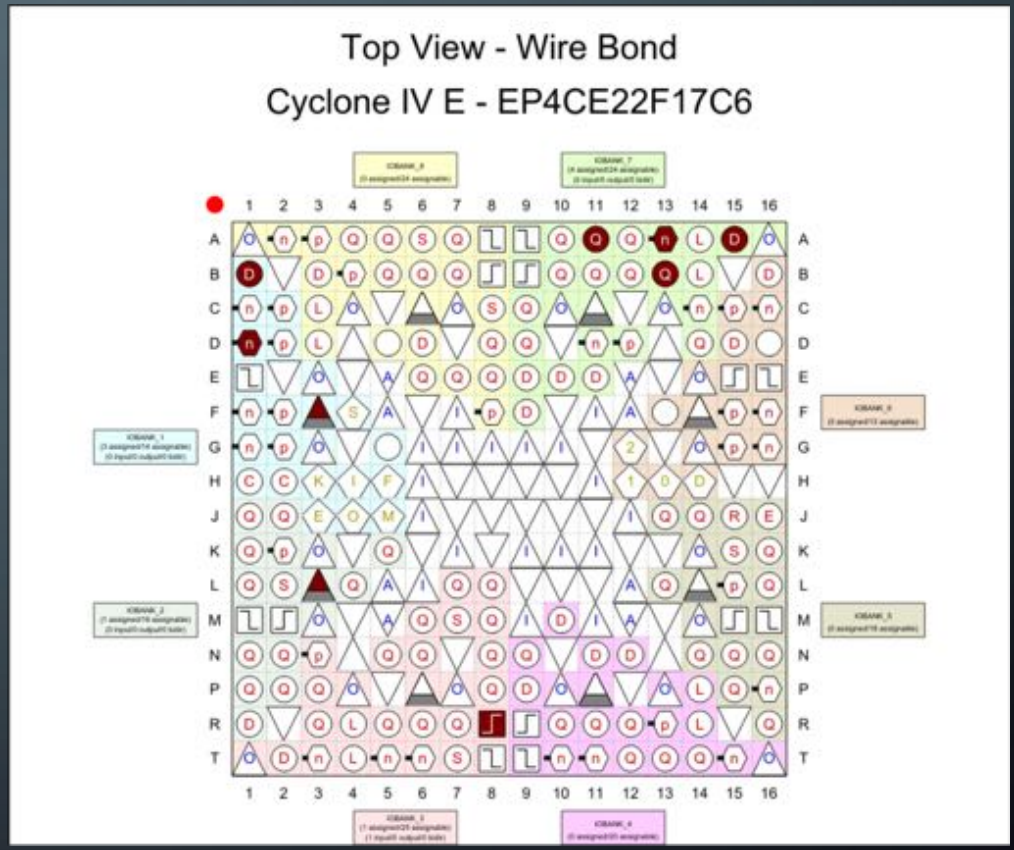
- Terasic DE0-Nano Cyclone FPGA
- < $100 22K LE FPGA board
- Quartus II Version 13.0.1 Web Edition (Linux)
- JTAG SignalTap II
- Verilog design & JSON scripts for getWork (no stratum)
- Hashrate 3-28MH/s (25 – 450MHz)

https://github.com/cryptodashie/Open-Source-FPGA-Bitcoin-Miner

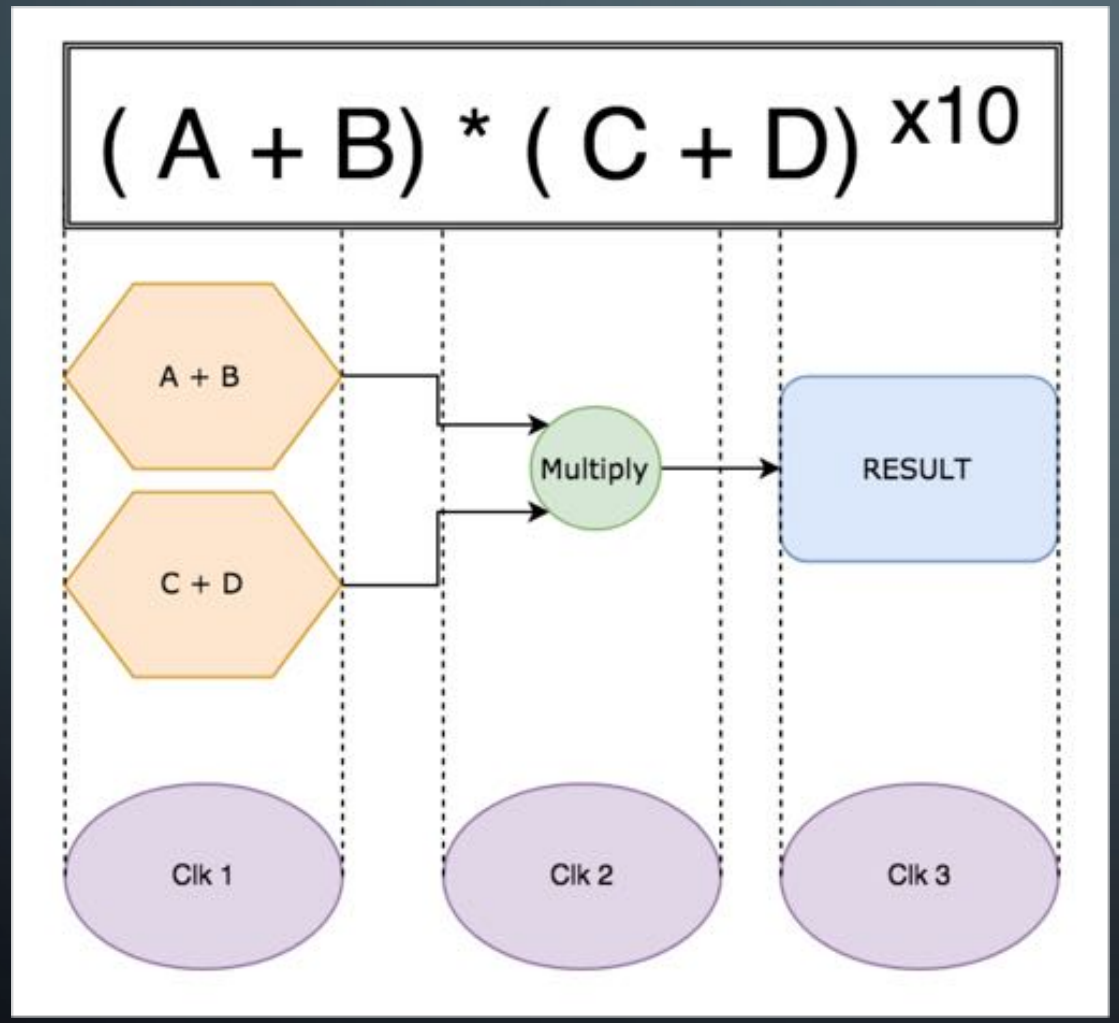


FPGA – DIGITAL DESIGN & MODELLING



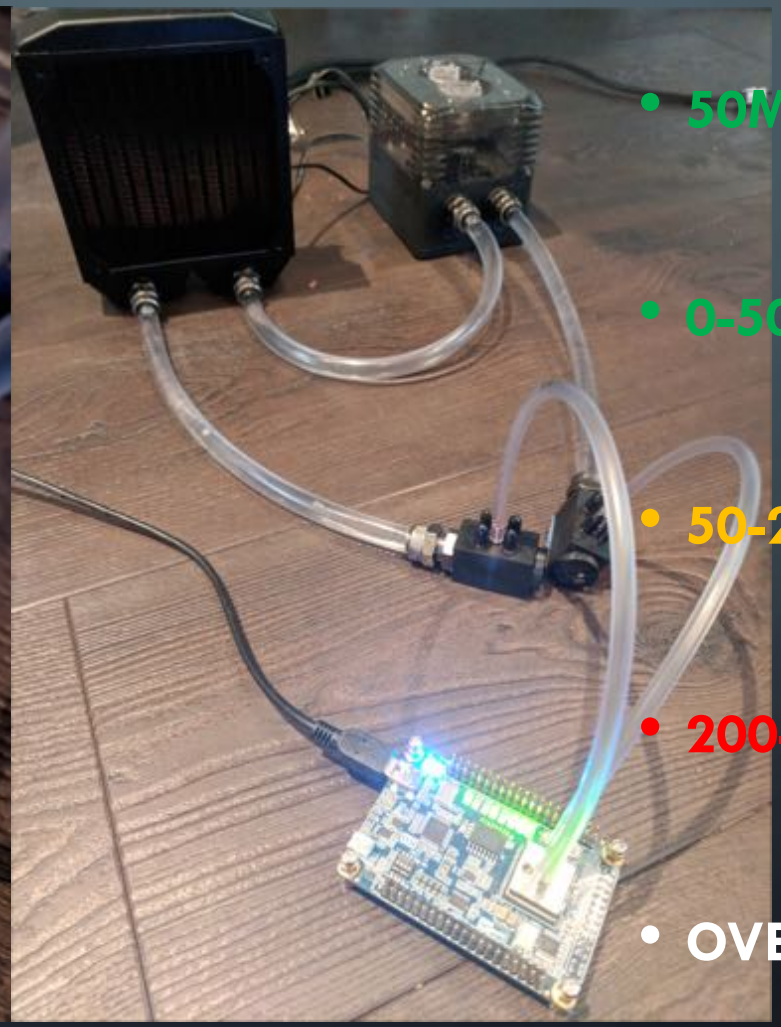


FPGA PIPELINING & PERFORMANCE ENHANCING IO



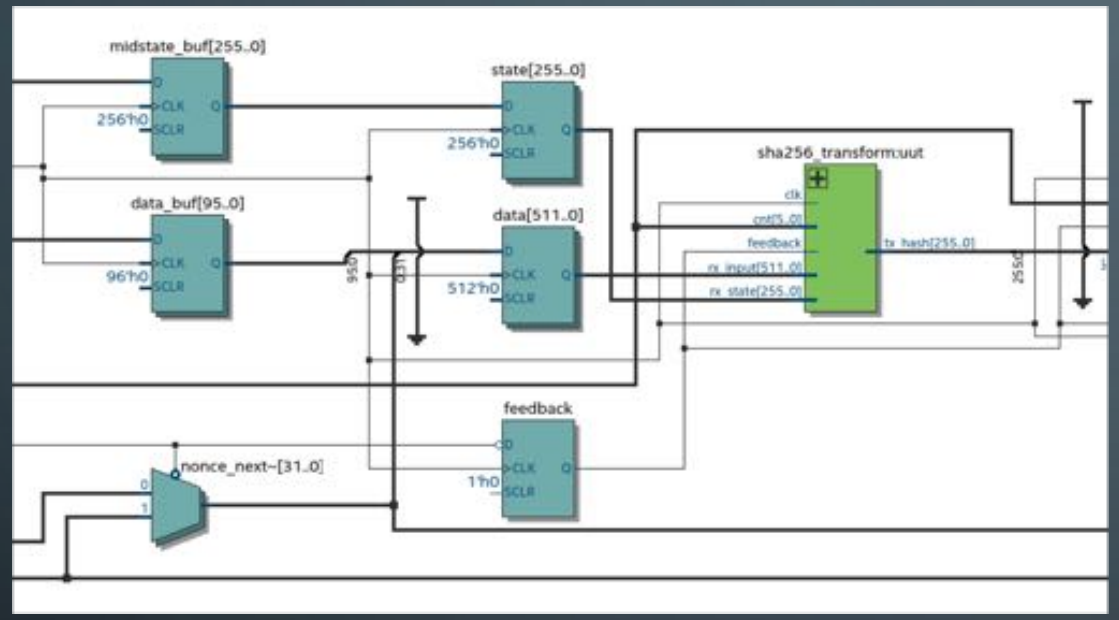
- Phase-locked Loop (PLL)
- High speed I/O (GPIO++)
- **Fast data transfer**
- **OVERCLOCK** ***DANGEROUS***

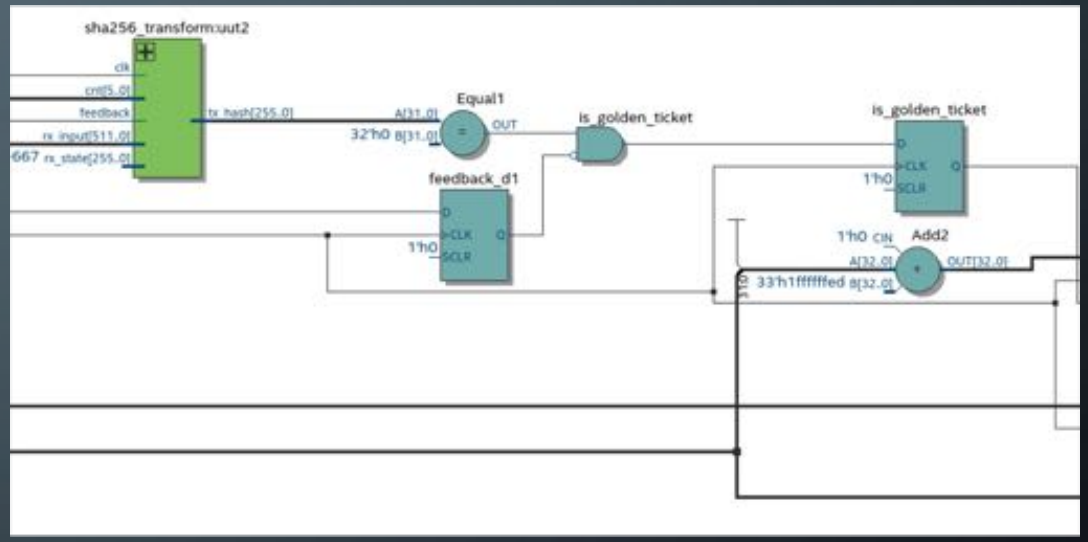
FPGA OVERCLOCKING & WATER COOLING

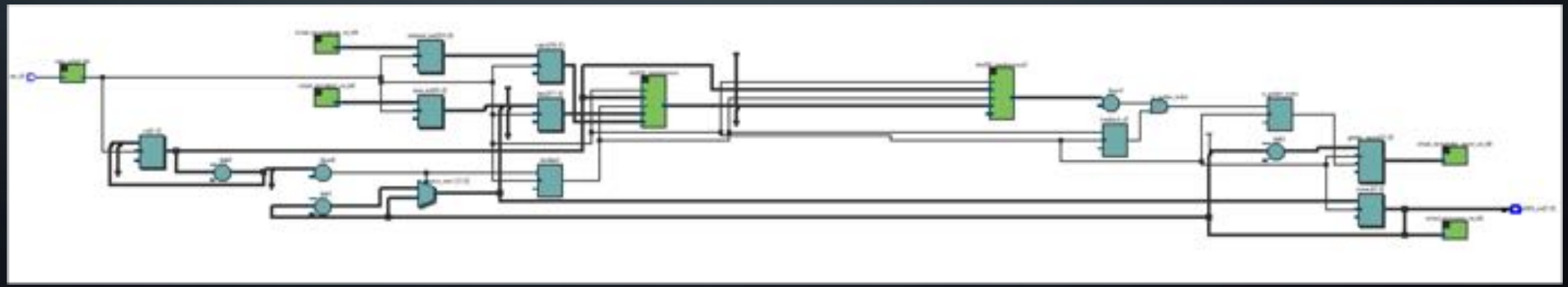


- 50MHz XTAL
- 0-50 MHz (no cooling)
- 50-200 MHz (fan/heatsink)
- 200-450 MHz (water)
- OVERCLOCK AT OWN RISK

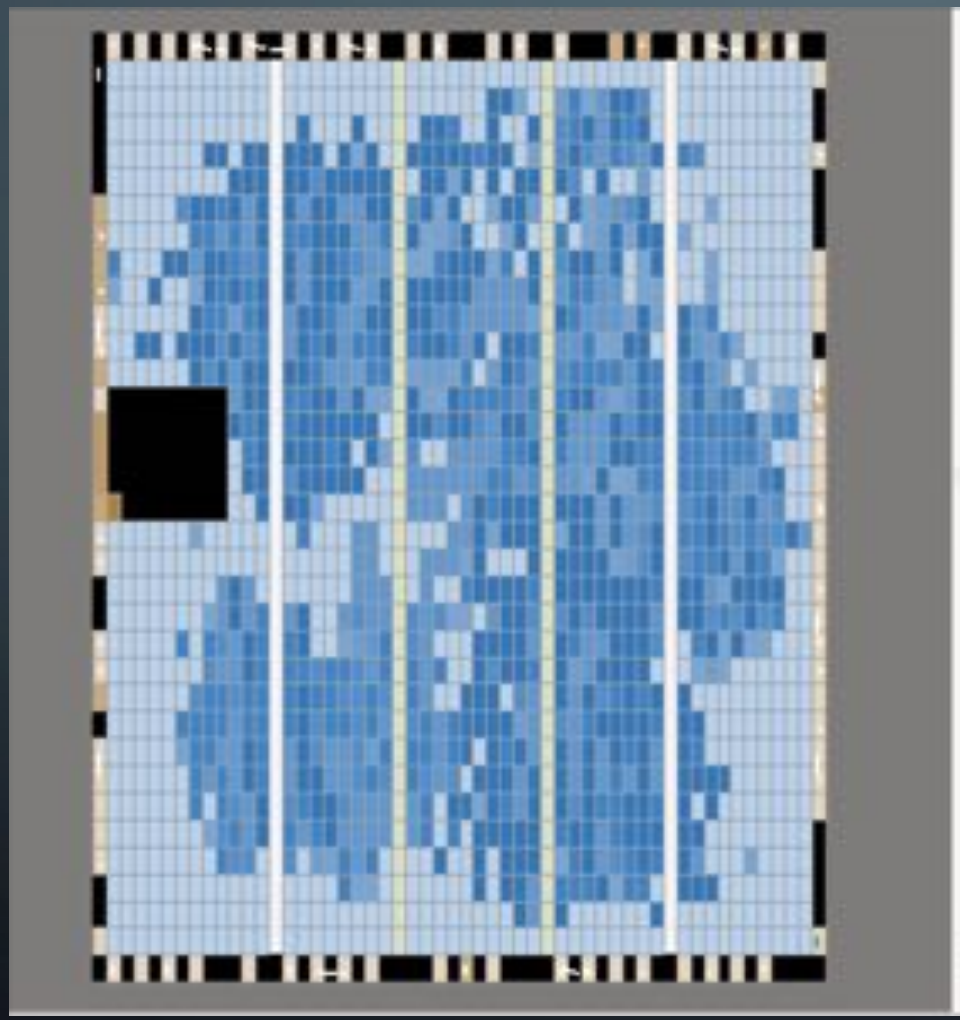
BITCOIN PROOF-OF-WORK BLOCK DIAGRAM







CHIP PLANNER BLOCK UTILIZATION



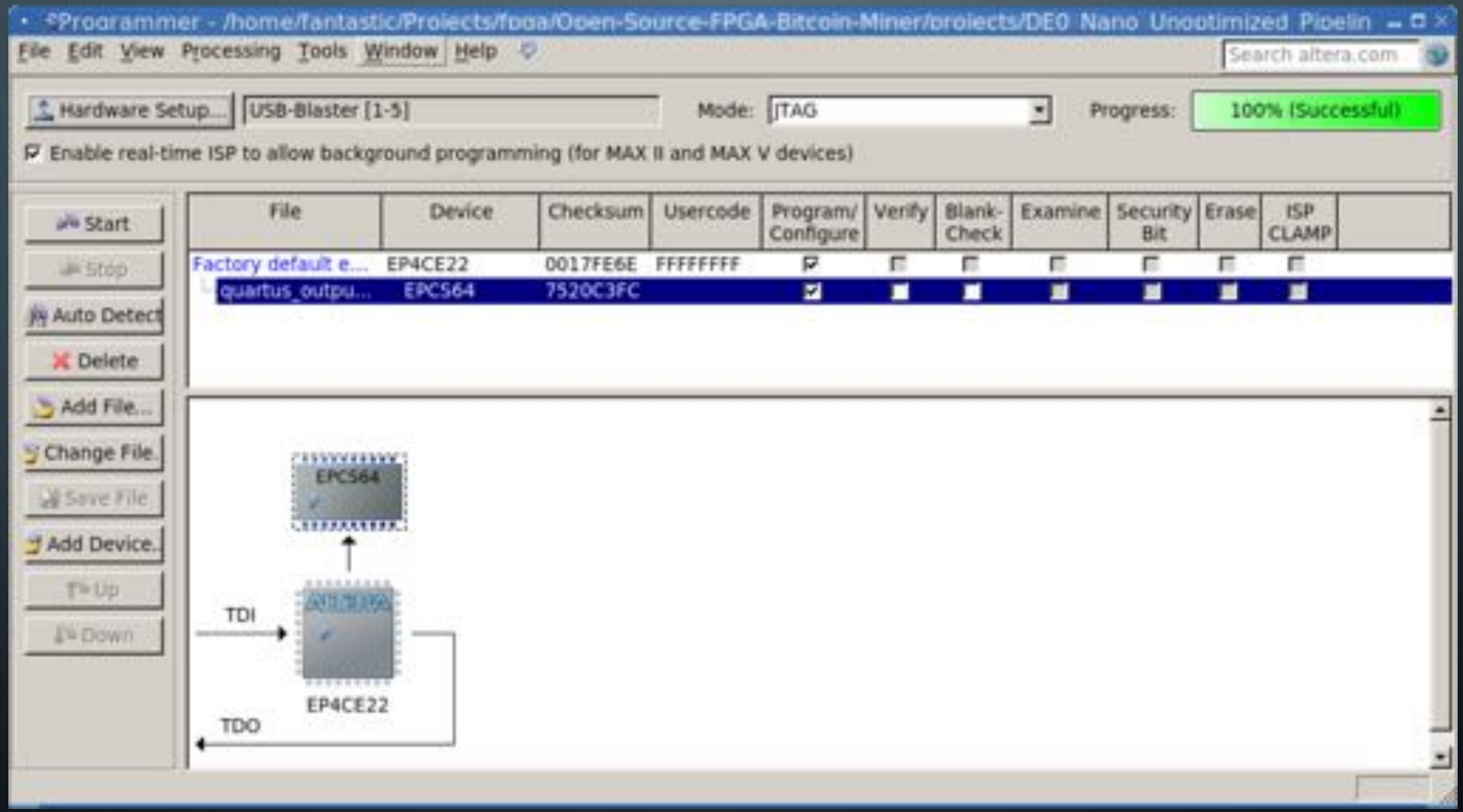
Selected elements:

General

Device	EP4CE22F17C6*
Family	Cyclone IV E
Device Extents	54 x 35
LEs	22320
Total I/Os	154
GPIOs	154
Memory Bits	608256
Embedded multiplier 9-bit elements	132
PLLs	4
Global Clocks	20

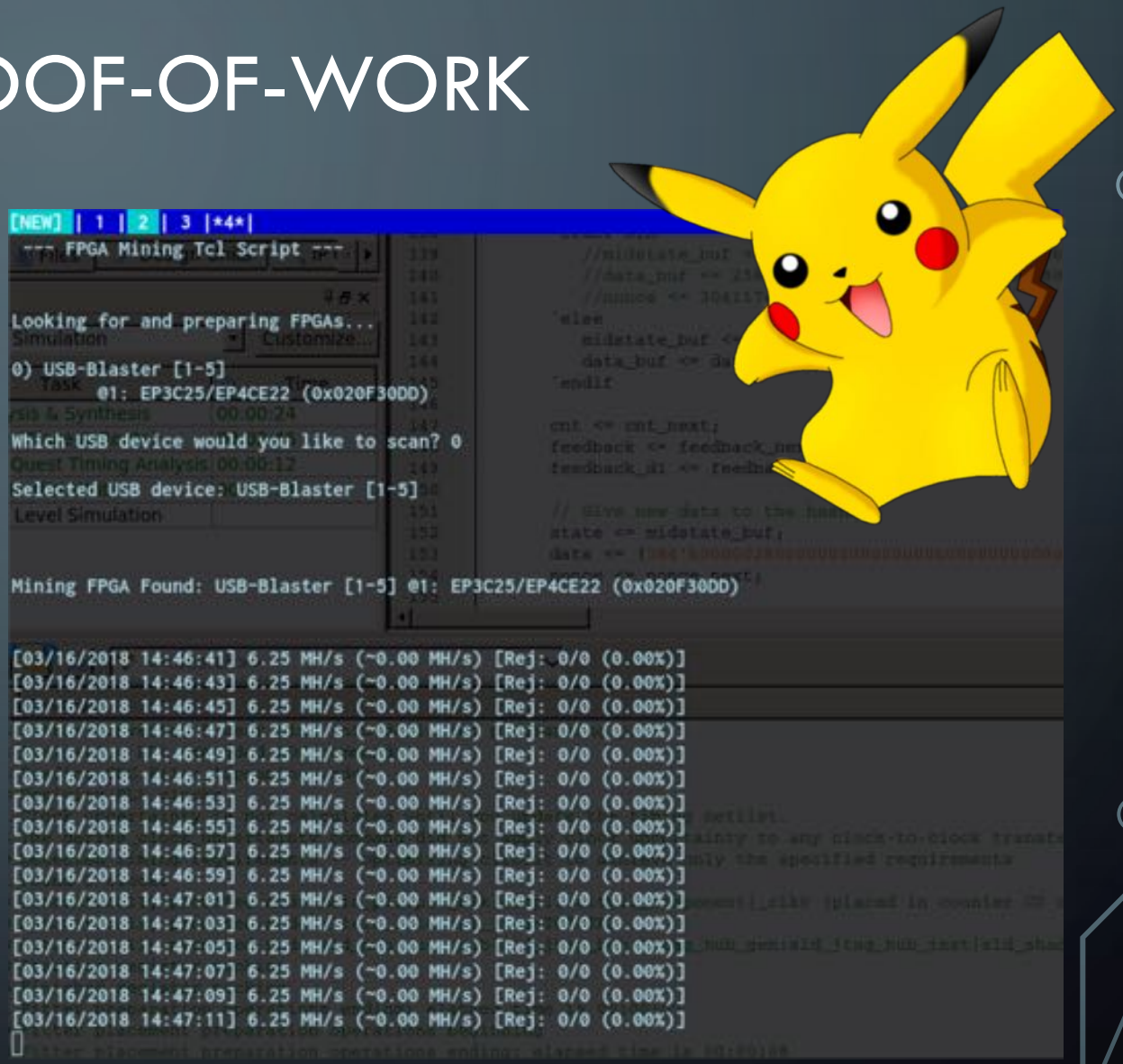
Device Properties | Layers Settings | Color Legend

FPGA PROGRAM DE0-NANO VIA FLASH LOADER



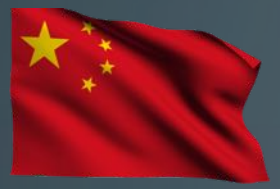
SCALABLE R&D FOR PROOF-OF-WORK ALGORITHMS

- Litecoin Core example available
- Pokemon your own!
- Keecak SHA-3? 1/2/3 from X11?



ASIC MINERS


zeus

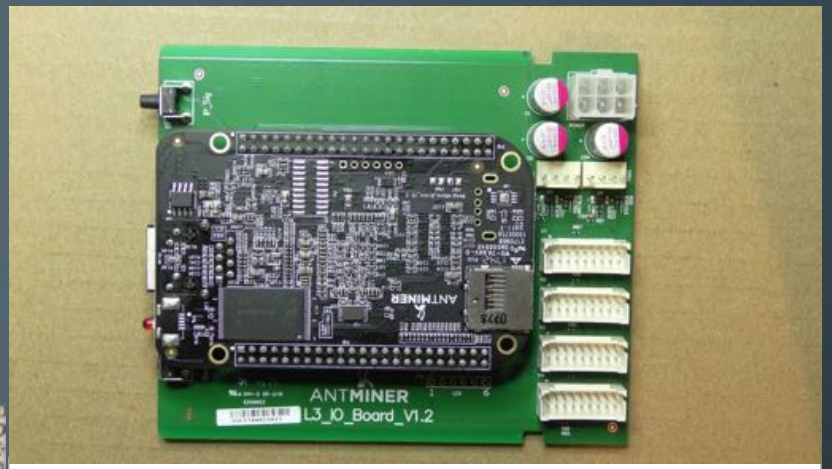


MADE IN CHINA, HACKED IN UK!

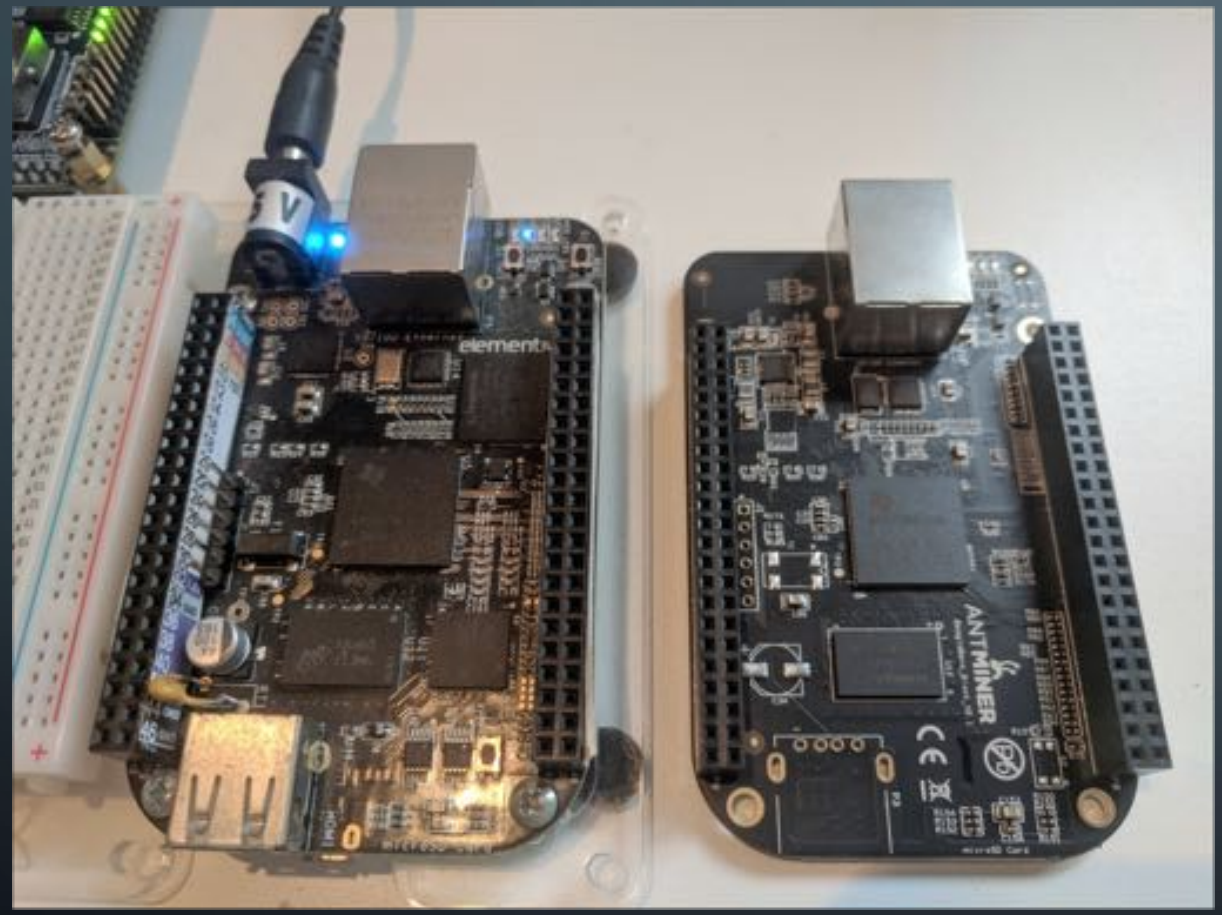
HEALTH HAZARDS, BE SAFE.

BITMAIN

ANTMINER



BEAGLECLONE – PARTIAL POPULATED BLACK PCB

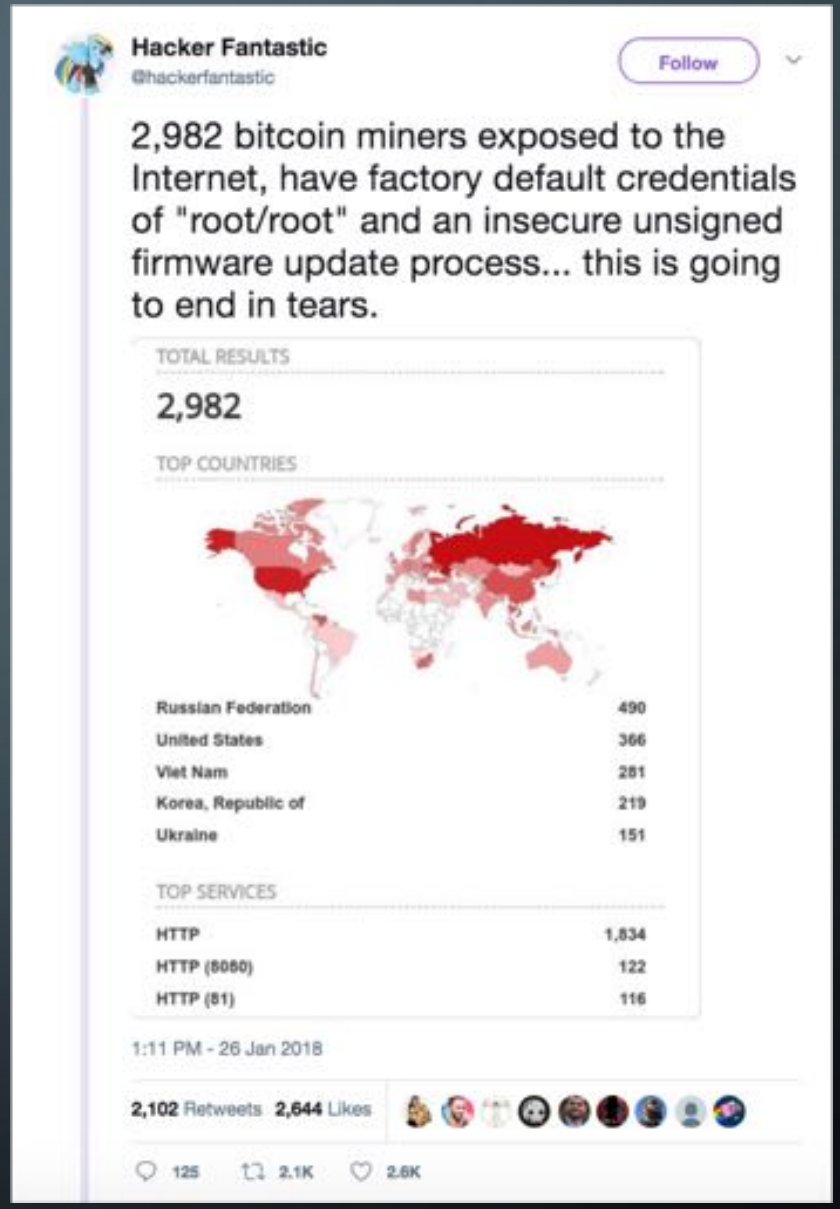


- *L3+ / A3 / D3* model controllers
- Angstorm Linux
- Firmware easily dumped / downloaded
- No code signing, trivial to mod
- **auth.minerlink.com** remote manager “antbleed” 🙄
- **SSH / HTTP defaults** **”root/root”** **“root/admin”**

SHODAN

HACKING BITCOIN MINERS

- Shodan / Google Dork to identify miners
- Easy strings “antMiner Configuration” realm
- Exposed footprint has Pre-Auth information leaks
- IP geolocate large remote mining farms



BITMAIN FIRMWARE HACKING

- https://github.com/cryptodashie/bitmain_hacking (reverse engineering data)

- 1.5% DEV FEE (pool switching)

- Blissz port cgminer-4.9 to cgminer-4.10

```
# updated to cgminer 4.10.0
--bitmain-reboot    Enable bitmain miner to reboot on low hashrate
--bitmain-reboot-asic Enable bitmain miner to reboot on high amount of ASIC fails
--bitmain-fan-mode <arg> Choose bitmain miner fan control mode 0 = auto, 1 = auto silent
, 2 = auto perf, 3 = manual mode (default: 0)
--bitmain-fan-pwm <arg> Set bitmain fan pwm percentage 0~100 (default: 10)
--bitmain-freq <arg> Set frequency (default: 100)
--bitmain-freq1 <arg> Set frequency chain 1 (default: 0)
--bitmain-freq2 <arg> Set frequency chain 2 (default: 0)
--bitmain-freq3 <arg> Set frequency chain 3 (default: 0)
--bitmain-core-temp <arg> Select core temp (default: 2)
--bitmain-voltage <arg> Set voltage (default: 600)
--bitmain-voltage1 <arg> Set voltage chain 1 (default: 0)
--bitmain-voltage2 <arg> Set voltage chain 2 (default: 0)
--bitmain-voltage3 <arg> Set voltage chain 3 (default: 0)
```

- Control individual boards in software, no need for hardware modifications (A++)

WAREZ JUAREZ REVOLUTION
SIACOIN/SIAFUND …

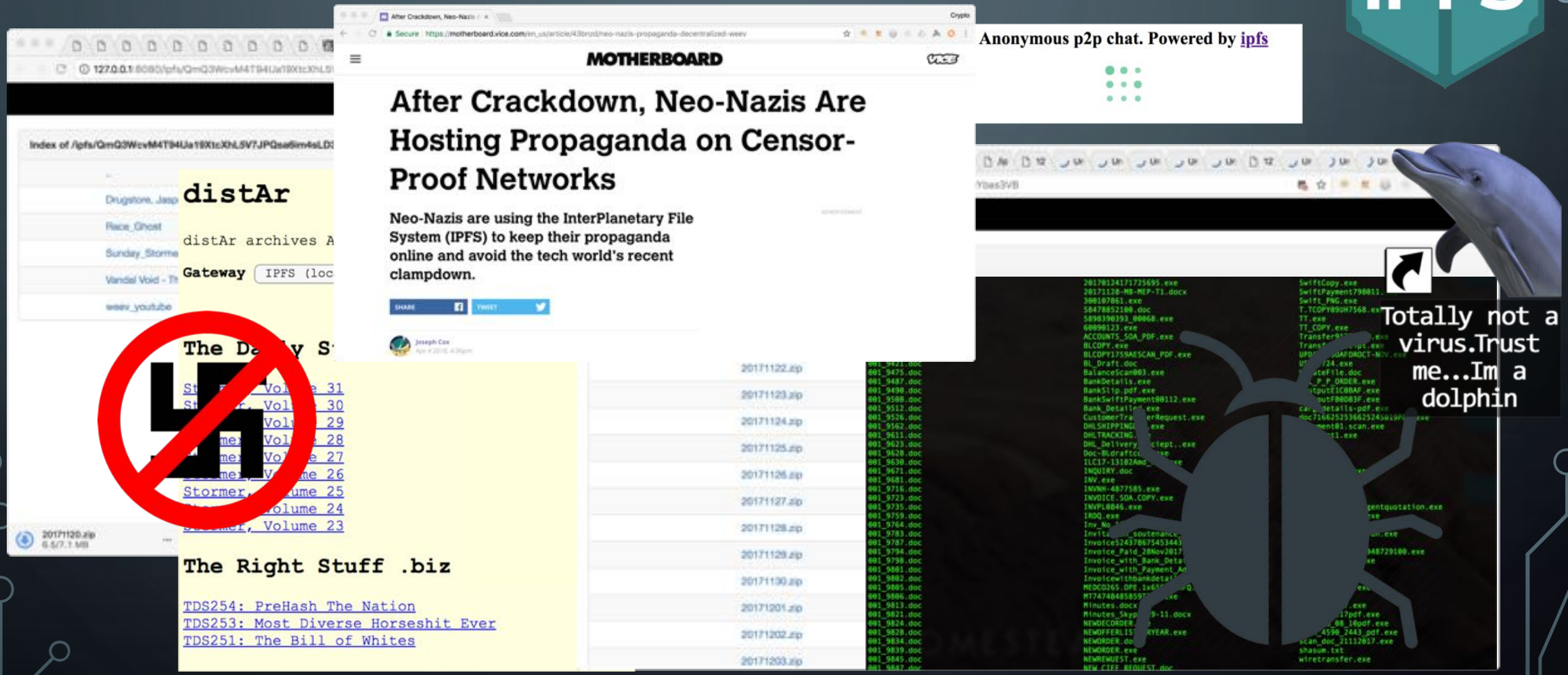
INTERPLANETARY FILE SYSTEM (IPFS)

http://ipfs.io/ (scan data) https://github.com/cryptodashie/ipfs


```
ipfs swarm peers | sed "s:.*/ipfs/\(.*\)\$:\1:g" | xargs -n1 -P5 ipfs name resolve > peers
cat peers | grep -v "/ipfs/QmUNLLsPACCz1vLxQVkXqqLX5R1X345qqfHbsf67hvA3Nn" | sed "s|^|http://127.0.0.1:8080|" | xargs open
```

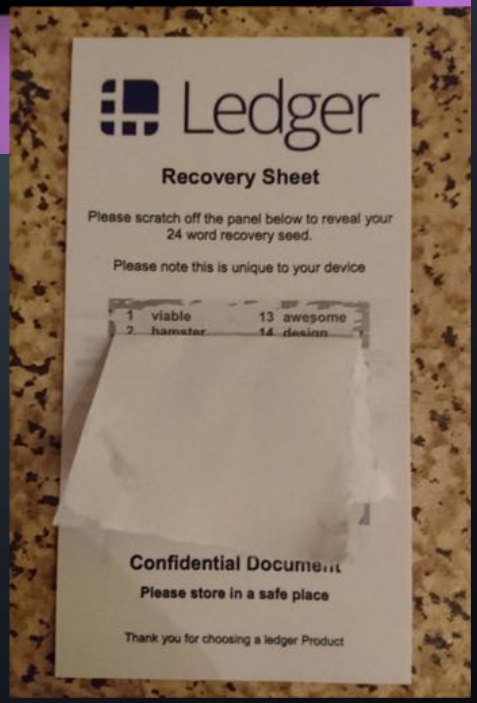
```
USAGE
  ipfs swarm - Interact with the swarm.

  ipfs swarm

  'ipfs swarm' is a tool to manipulate the network swarm. The swarm is the
  component that opens, listens for, and maintains connections to other
  ipfs peers in the internet.

SUBCOMMANDS
  ipfs swarm addrs                    - List known addresses. Useful for debugging.
  ipfs swarm connect <address>...     - Open connection to a given address.
  ipfs swarm disconnect <address>...  - Close connection to a given address.
  ipfs swarm filters                  - Manipulate address filters.
  ipfs swarm peers                    - List peers with open connections.

Use 'ipfs swarm --help' for more information about this command.
```

HOSTS NEONAZIS, MALWARE, PORN, BLOGS...



HARDWARE WALLETS

- Hardware + Firmware
- Supply chain attacks
- All three platforms had recent patches, props Saleem Rashid!
- Chrome WebUSB (?)



WEB3.JS – ENUMERATION & PROMISE EXAMPLE

Enumerate account details, interact with wallets or prompt unlocking….

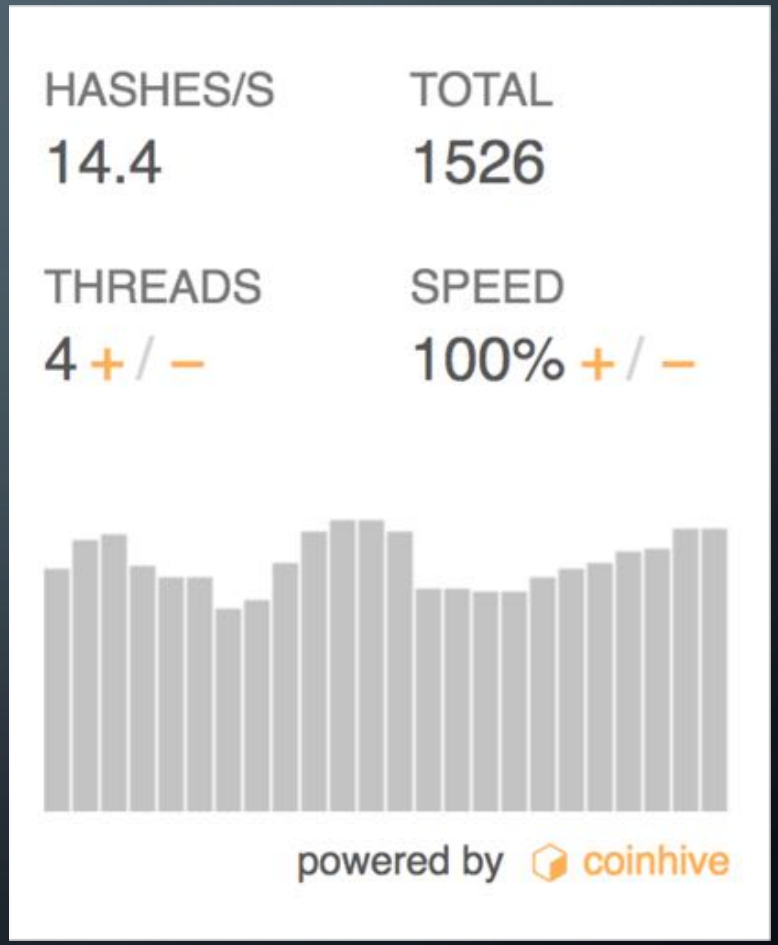
ethereum.js

```
var Web3 = require('web3');
var web3 = new Web3(Web3.givenProvider || 'http://localhost:8545');
var globalaccount;
web3.eth.getAccounts().then(querybalance);

function querybalance(accounts){
  if(accounts.length > 0){
    for(var index = 0;index < accounts.length;index++){
      globalaccount = accounts[index];
      console.log(accounts[index]);
      var balance = web3.eth.getBalance(accounts[index],web3.eth.defaultBlock,sendfunds);
    }
  }
}
```

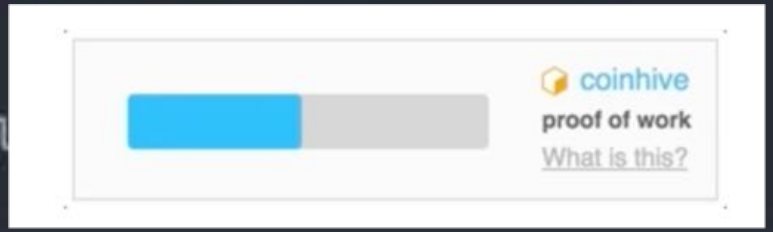
While it's possible to run the miner without informing your users, we strongly advise against it. You know this. Long term goodwill of your users is much more important than any short term profits.

RISE OF THE CRYPTONIGHT JAVASCRIPT MINER

- Cryptonight proof-of-work can mine Monero (XMR)
- Replace captchas, adverts or monetize links
- Very low profit returns, $0.1 (users adapt)



```
<script src="https://authedmine.com/lib/captcha.min.js" async></script>
<script>
function CaptchaCallback(token) {
    var x = document.getElementsByClassName("wpcf7-form");
        x[0].submit();
}
</script>
<font color="black"><bold>We use a proof-of-work javascript mining
algorithm instead of a captcha to validate humans. Click verify me and
wait to submit the form.<bold></font>
<div class="coinhive-captcha" data-hashes="1024" data-key="<KEYHERE>"
data-whitelabel="true" data-disable-elements='input[type="submit"]'
data-callback="CaptchaCallback" >
<em>Loading Captcha...<br>
If captcha doesn't load, please disable adbl
</div>
```



INTERNET-OF-THINGS, PUBLIC SPACE, SHORT LINKS

MONERO-IN-THE-MIDDLE (XMR INJECTION)

- Use of WiFi enabled embedded device
- KARMA attack (hostapd-wpe)
- PAYG Internet Connectivity via (4G) LTE
- Supports multiple MITM modes of operation

Starbucks customer laptops hacked to mine cryptocurrency

- Twitter user points out that a store in Buenos Aires had corrupted Wi-Fi
- Reports claim illegal script was using customer laptops to mine Monero coins
- The coffee chain says the internet connection has now been made safe

DEMO

RECOMMENDED READING

- Verilog by example - Blaine C. Readler
- Mastering Bitcoin – Andreas Antonopoulos
- Introducing Ethereum and Solidity - Chris Dannen

hacker.house | Hacker House

Hacker House

EXCLUSIVE HACKER HOUSE PRODUCTS

bitcoin
ACCEPTED HERE

Q&A?

THANK YOU #COINFESTUK FOR LISTENING

https://hacker.house