

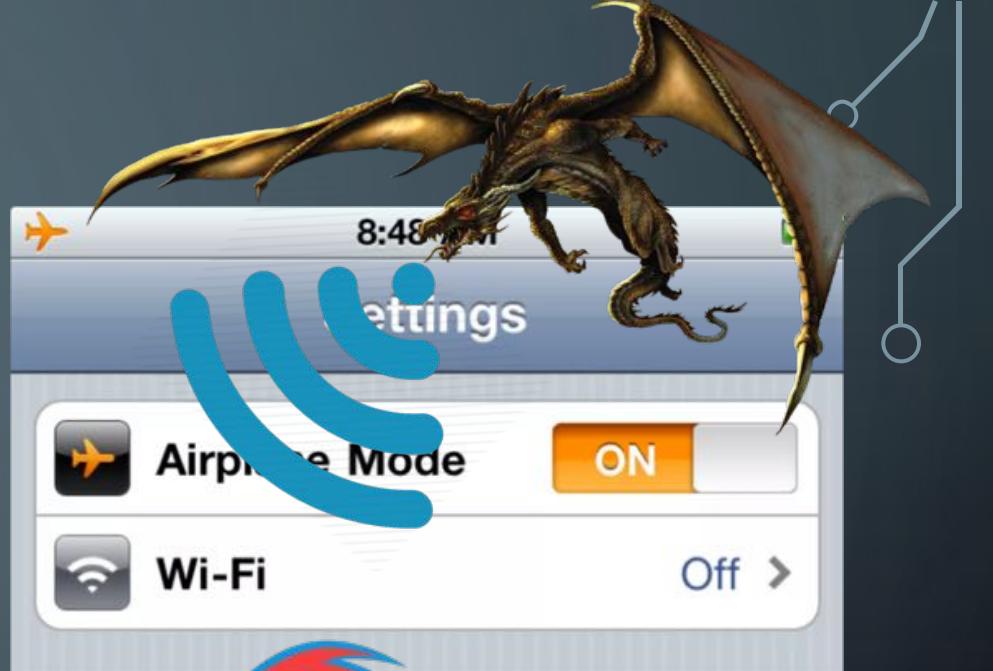


HACKER H O U S E

A BLOCKCHAIN QUEST

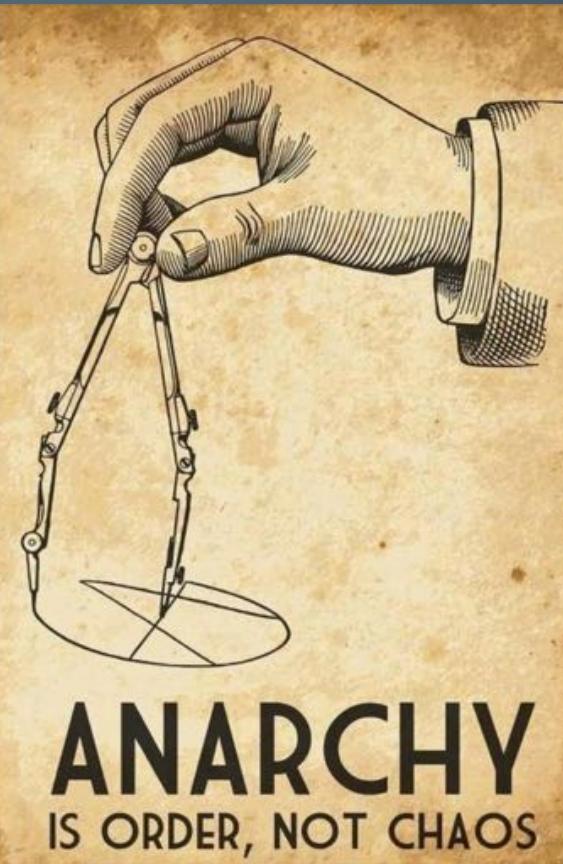
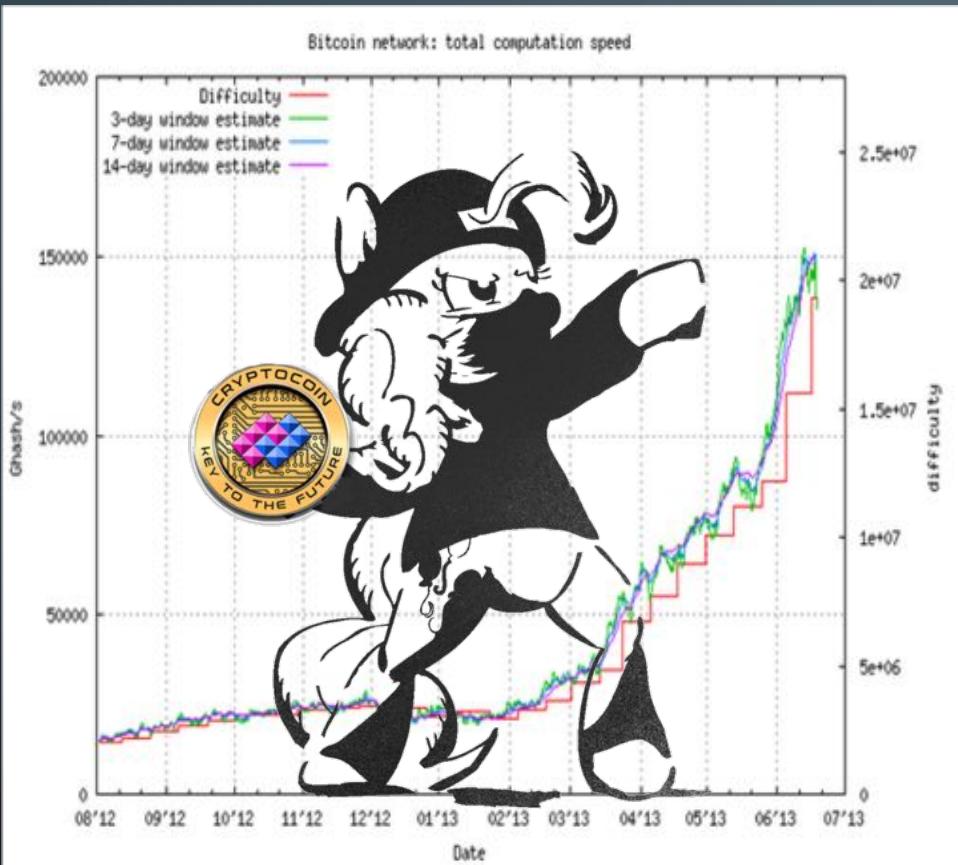
INTRODUCTIONS

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



A

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

Hackers steal \$64 million from NEM



Technology Intelligence

Coincheck hackers trying to move stolen cryptocurrency after major Japanese heist



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



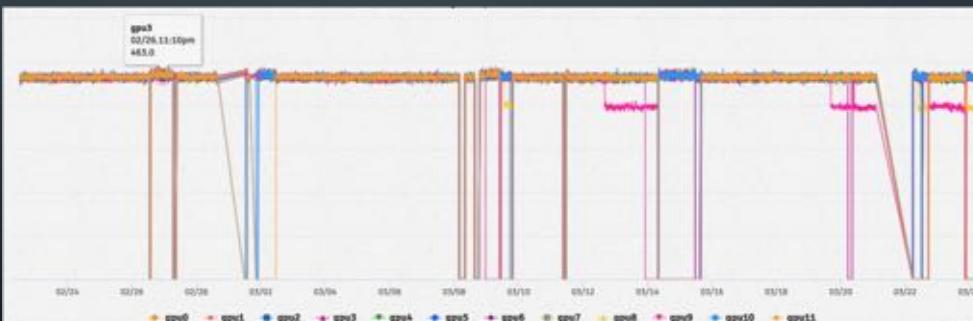
YOU ENTER THE TAVERN...

- 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!





GPU ...



**CHOOSE YOUR
CHARACTER**

... FPGA



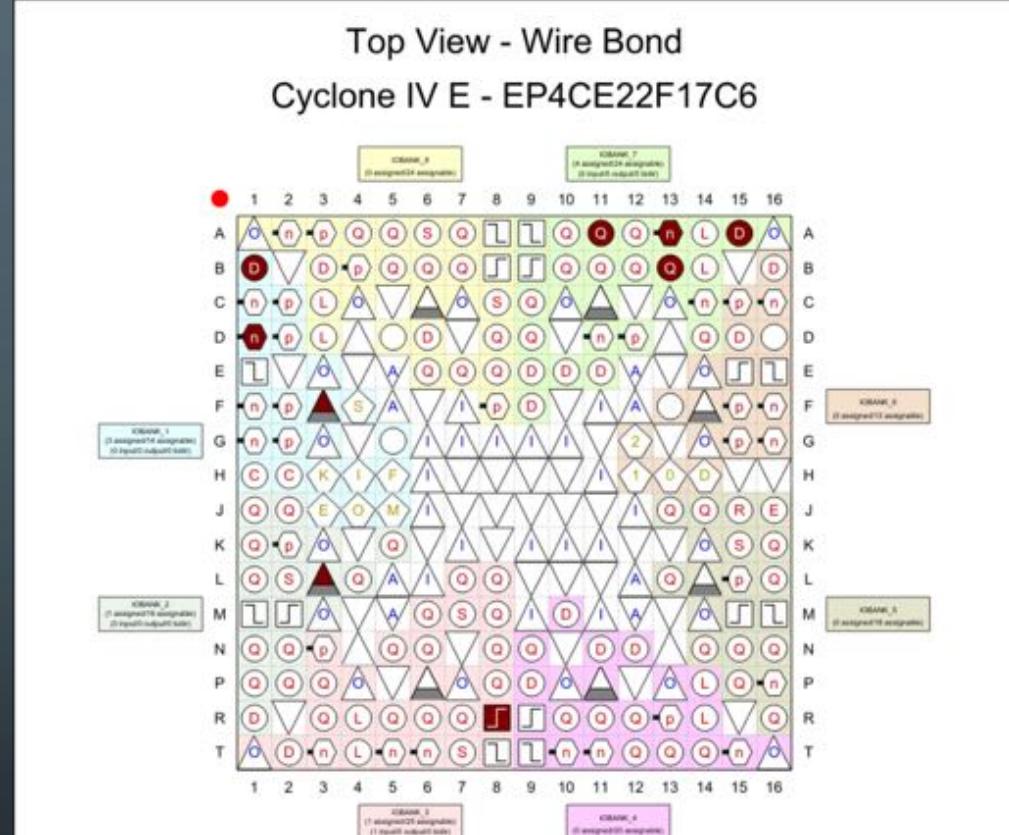
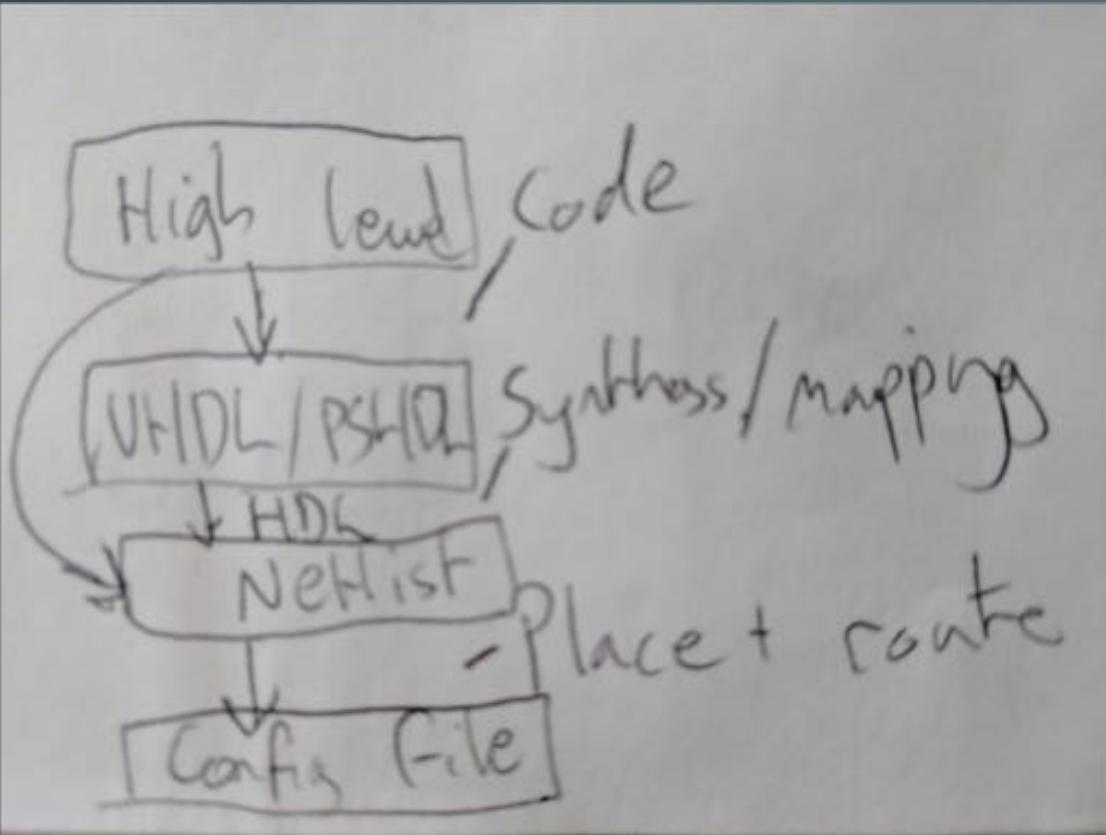
DEVELOPMENT BOARD

- 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)

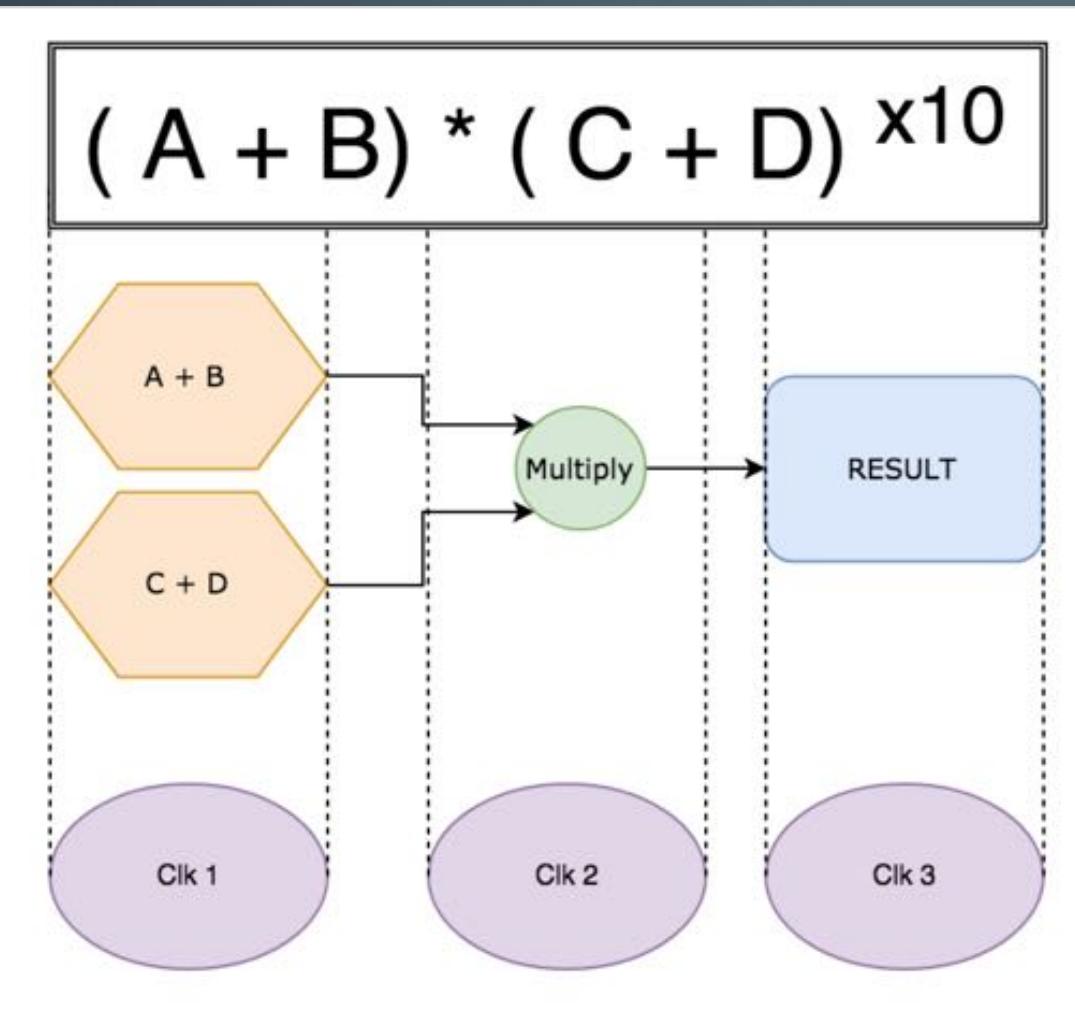
<https://github.com/cryptodashie/Open-Source-FPGA-Bitcoin-Miner>



FPGA – DIGITAL DESIGN & MODELLING

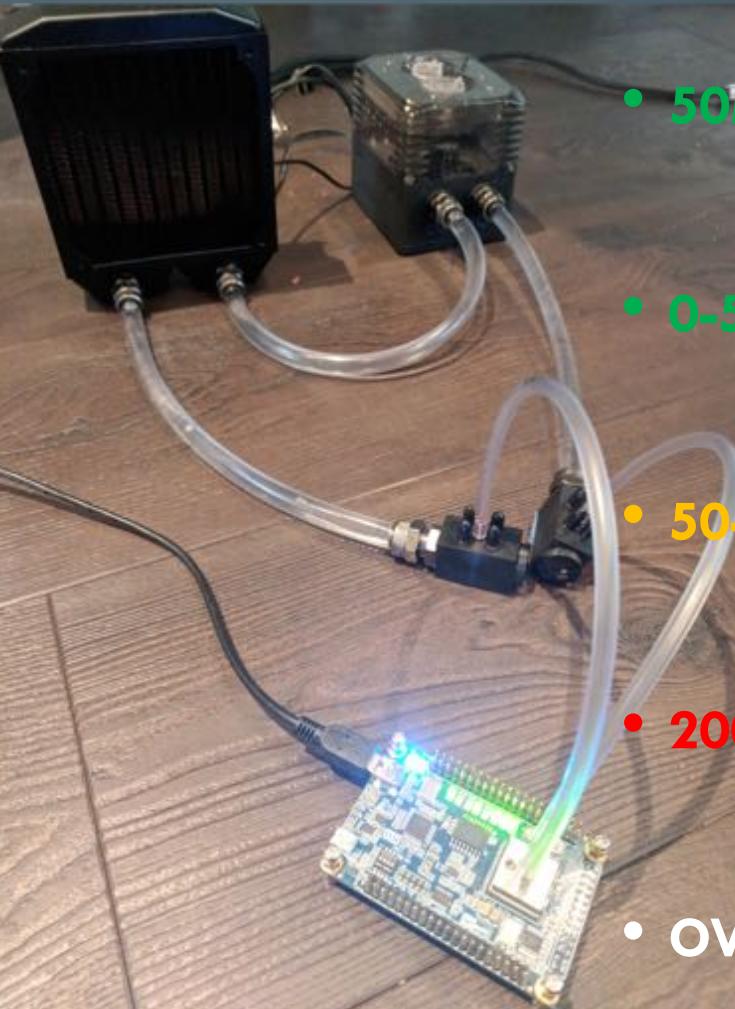
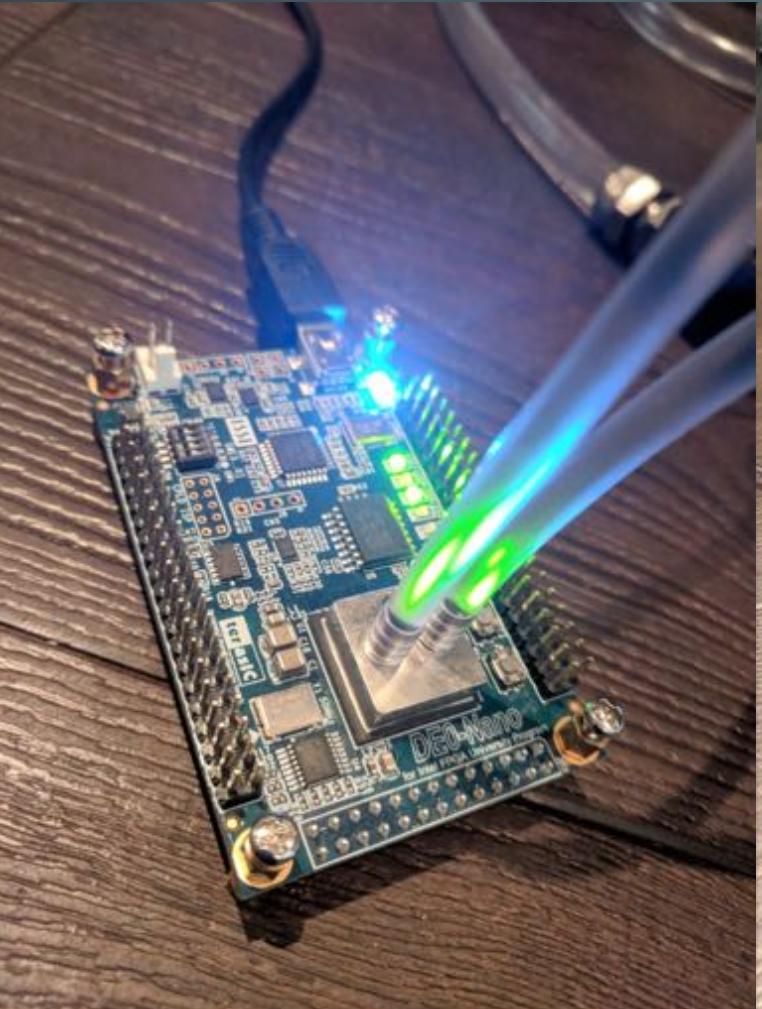


FPGA PIPELINING & PERFORMANCE ENHANCING IO



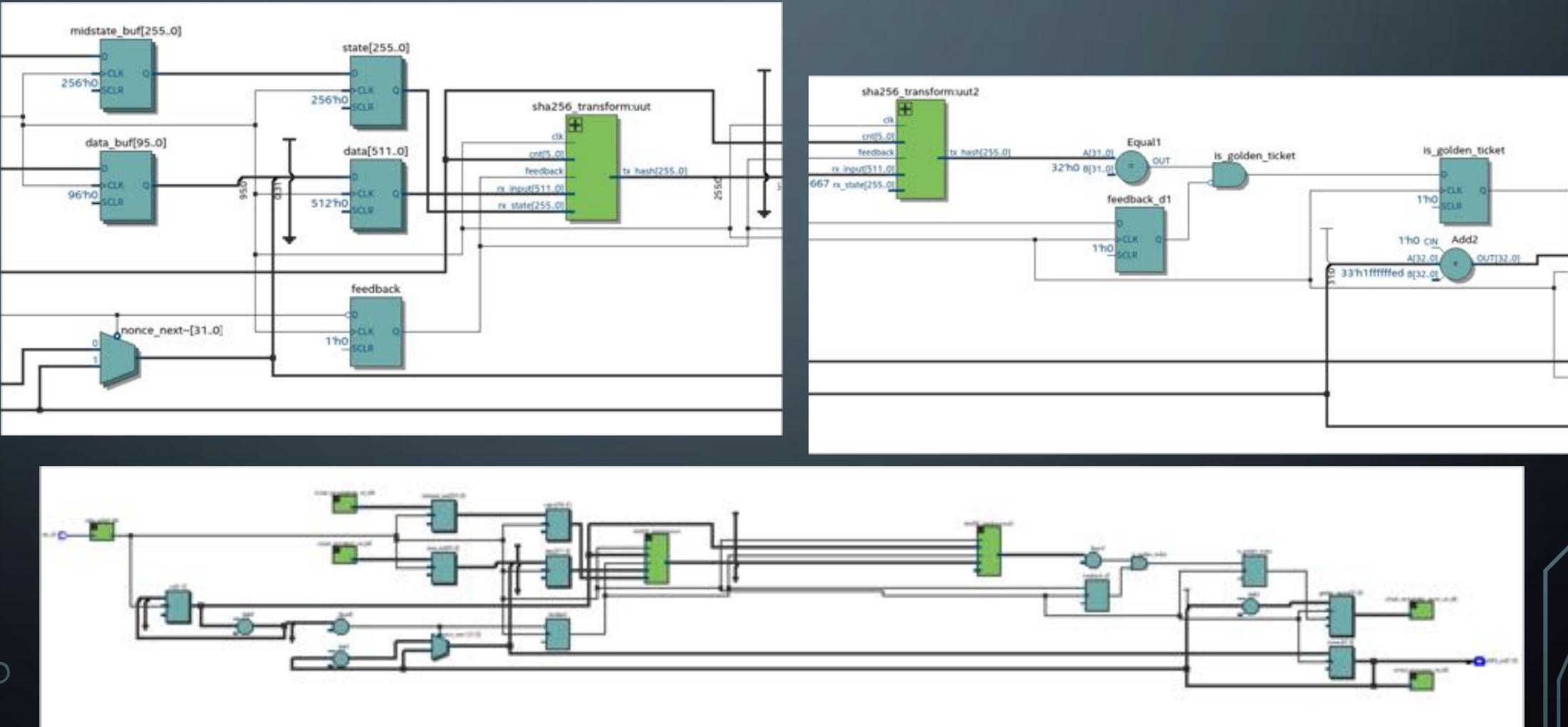
- Phase-locked Loop (PLL)
- High speed I/O (GPIO++)
- Fast data transfer
- **OVERCLOCK *DANGEROUS***

FPGA OVERCLOCKING & WATER COOLING

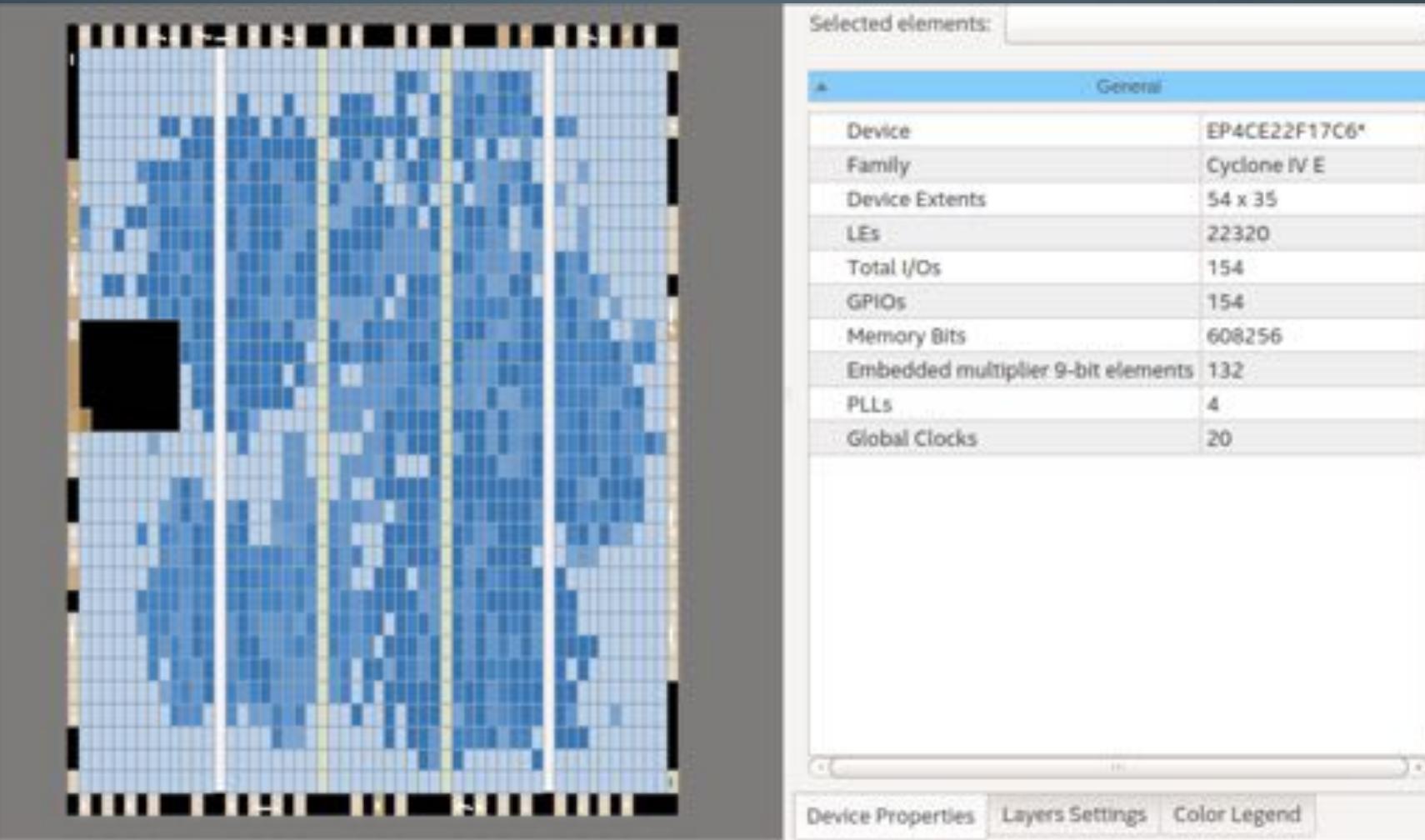


- **50MHz XTAL**
- **0-50 MHz (no cooling)**
- **50-200 MHz (fan/heatsink)**
- **200-450 MHz (water)**
- **OVERCLOCK AT OWN RISK**

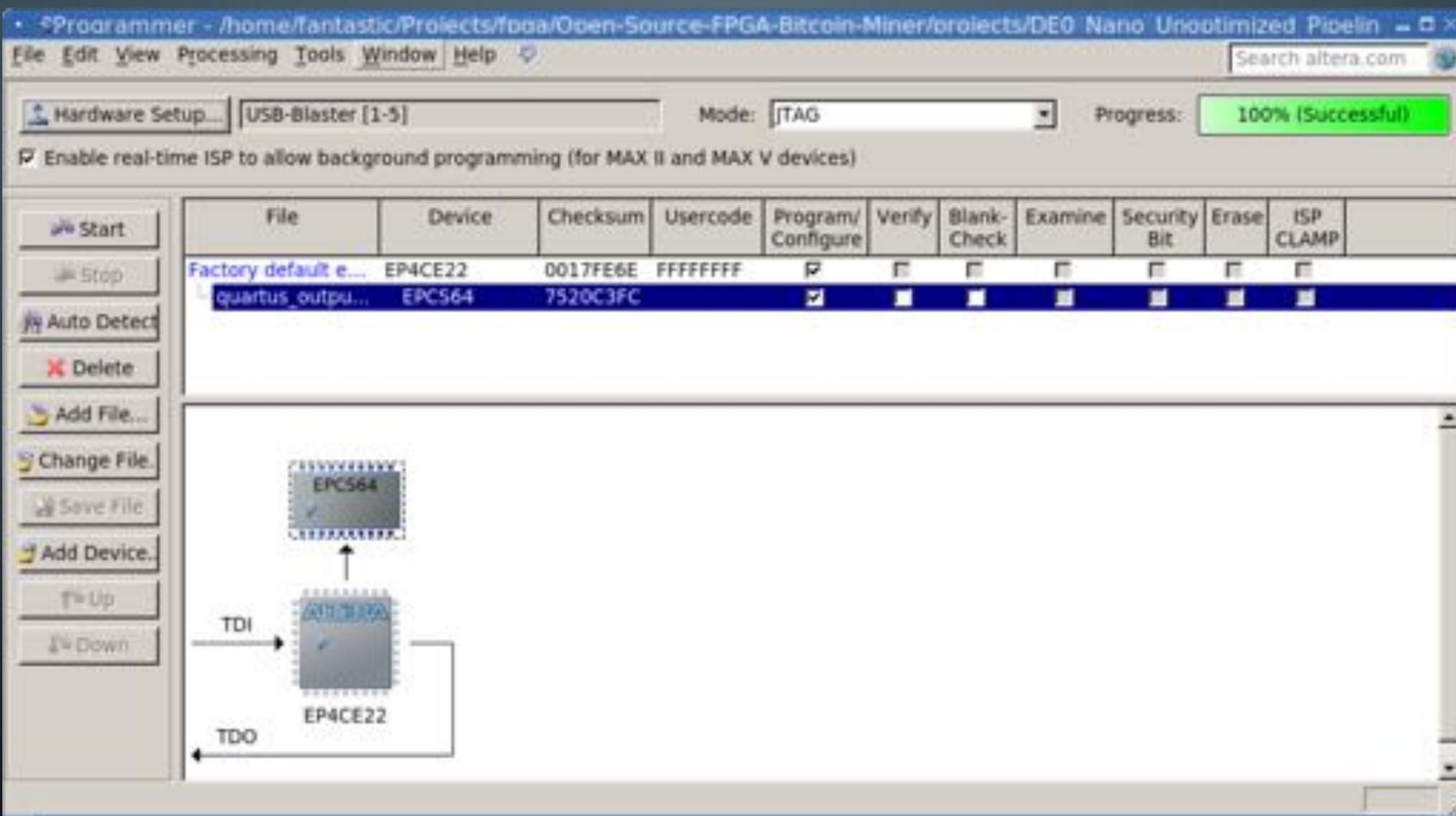
BITCOIN PROOF-OF-WORK BLOCK DIAGRAM



CHIP PLANNER BLOCK UTILIZATION



FPGA PROGRAM DEO-NANO VIA FLASH LOADER



SCALABLE R&D FOR PROOF-OF-WORK ALGORITHMS

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



The image shows a terminal window titled "FPGA Mining Tcl Script" with the following content:

```
[NEW] | 1 | 2 | 3 | *4* | --- FPGA Mining Tcl Script ---  
Looking for and preparing FPGAs...  
Simulation      Customize  
0) USB-Blaster [1-5]      01: EP3C25/EP4CE22 (0x020F30DD)  
Synthesis      00:00:24  
Which USB device would you like to scan? 0  
Gate Timing Analysis 00:00:12  
Selected USB device: USB-Blaster [1-5]  
Level Simulation  
Mining FPGA Found: USB-Blaster [1-5] 01: EP3C25/EP4CE22 (0x020F30DD)
```

Below the terminal window, there is a log of mining activity:

```
[03/16/2018 14:46:41] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:43] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:45] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:47] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:49] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:51] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:53] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:55] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:57] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:46:59] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:01] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:03] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:05] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:07] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:09] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]  
[03/16/2018 14:47:11] 6.25 MH/s (~0.00 MH/s) [Rej: 0/0 (0.00%)]
```

ASIC MINERS







MADE IN CHINA, HACKED IN UK!



HEALTH HAZARDS, BE SAFE.



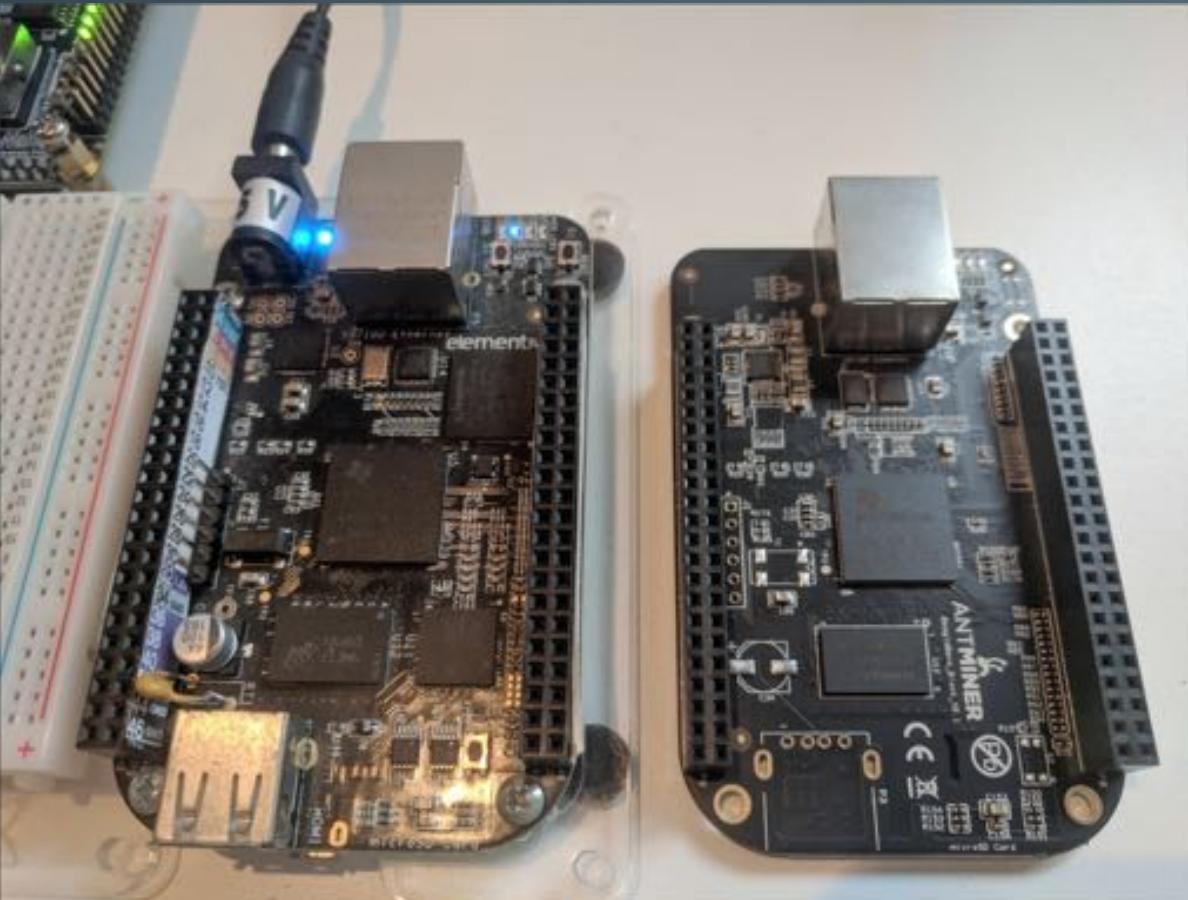
BITMAIN



ANTMINER



BEAGLECLONE – PARTIAL POPULATED BLACK PCB



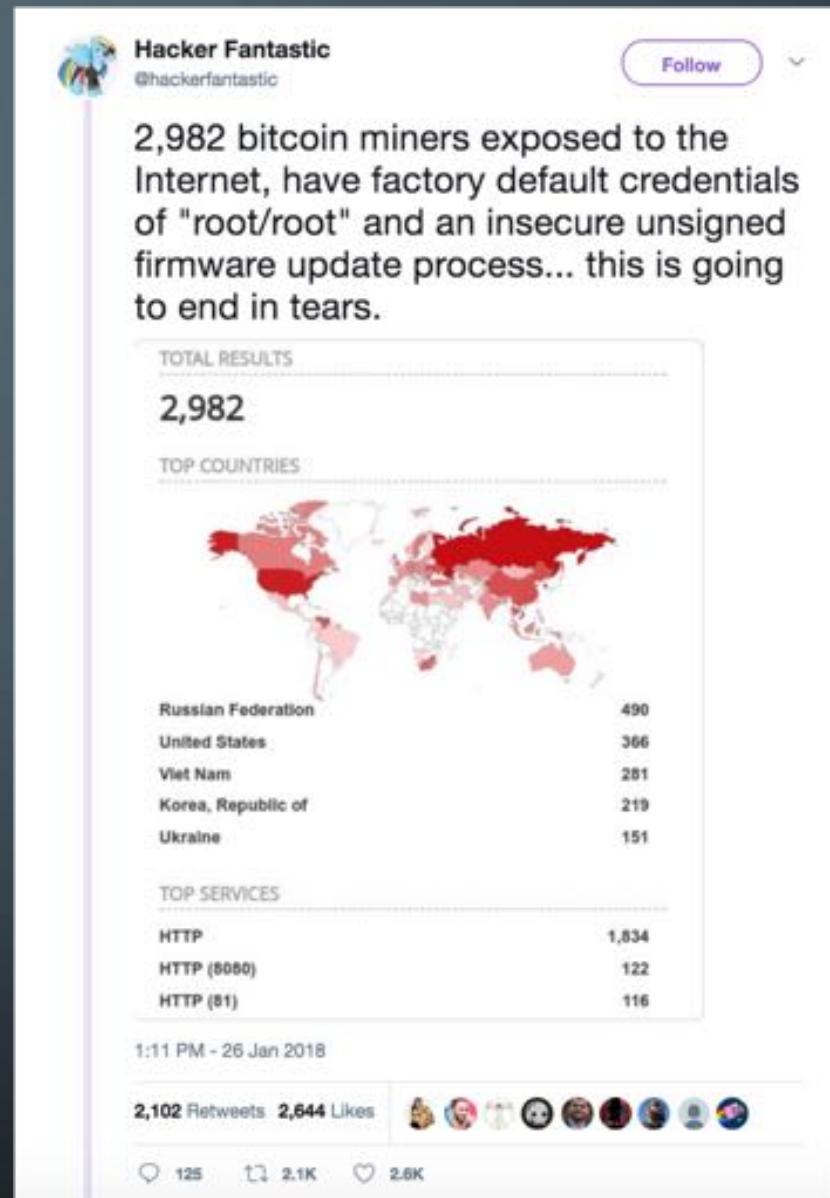
- L3+ / A3 / D3 model controllers
- Angstrom Linux
- Firmware easily dumped / downloaded
- No code signing, trivial to mod
- **auth.minerlink.com** remote manager
“antbleed”
- **SSH / HTTP defaults “root/root” “root/admin”**



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



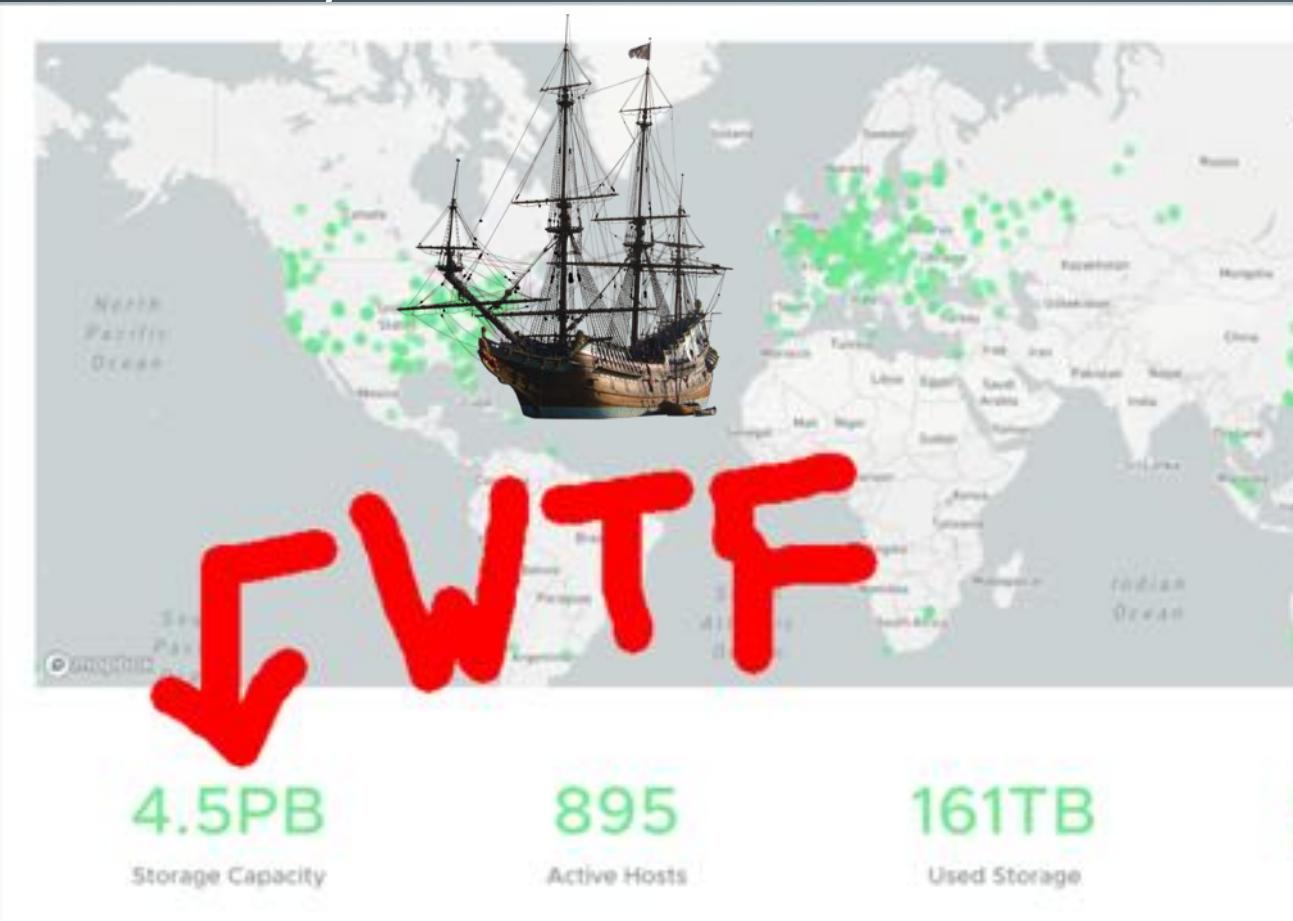
- https://github.com/cryptodashie/bitmain_hacking (reverse engineering data)

- 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>

```
1 ipfs swarm peers | sed "s:.*ipfs/(.*):\$:1:g" | xargs -n1 -P5 ipfs name resolve > peers
2 cat peers | grep -v "/ipfs/QmUNLLsPACCz1vLxQVkJXqqLX5R1X345qqfHbsf67hvA3Nn" | 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.

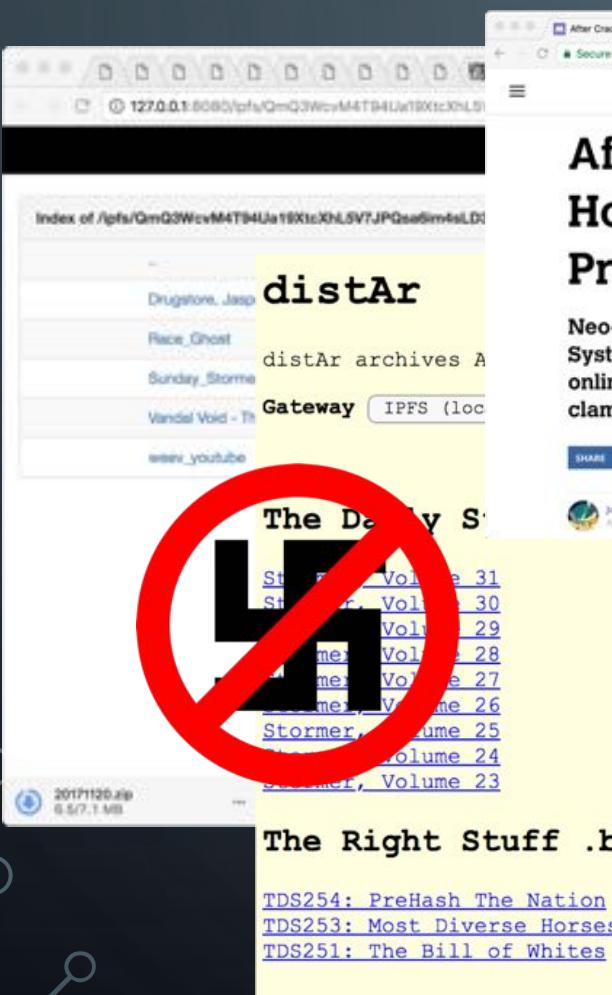
  Use 'ipfs swarm --help' for more information about this command.
```



seen discovered by crawling the swarm of a connected
node using the name resolver:

- <https://ipfs.io/ipfs/QmRLCKENKVJB5t8tWgxEWvF7RxyuA2huH5a/> Hello IPFS and Mark
- <https://ipfs.io/ipfs/QmRR16PF8M2ghXH8tUeVXHG2Qrx3j50D/> huoip (chinese social network)
- <https://ipfs.io/ipfs/QmRS4Cux38PK8efyB5qm9D5iHW8eCrutZ2J/> adult (XXX)
- <https://ipfs.io/ipfs/QmWUJenMeHgv16Vsaf8je1CcUHWQEONIC/> Coincidence detector
- <https://ipfs.io/ipfs/QmS5tVbz2jYGIugTMaRFgtxYKaWq4PjPvxd/> Miles boobs stuff
- <https://ipfs.io/ipfs/QmrrWbMy8wyVCmo65RA4CdFw0ymPAT5AG/> Troy's Tools <https://merchandise.troy.com/>
- <https://ipfs.io/ipfs/QmT84lgYkdhsrmssuFWiQmAdoTRUJAxhX5d/> blog french
- <https://ipfs.io/ipfs/QmSuDCam73pcm5vGKcSWmQd5d6oIqMq3/> hashes of images to movies (1)
- <https://ipfs.io/ipfs/QmQ3WcvM4T9Ua790zkhL5V7/PQsallQWk/> III NEONAZIS III
- <https://ipfs.io/ipfs/Qmf1Etwpdhg971UM9yj01BuCeh2AVisv4/> crypto
- <https://ipfs.io/ipfs/QmV8Wek5K0xbHsAehnkJtUobNmijg1UxP5/> media (mp3 music?)
- <https://ipfs.io/ipfs/QmXm1M2hdtskUz1fphzYUjNt55ppGzF4Isthmus/> is an experimental linux system
- <https://ipfs.io/ipfs/QmdnEiEF52vtnFilogn9svlCkqwehnRb49mlbjxYtq483V8U/> !!!!! MALWARE LOTS OF MALWARE!!!!
- <http://gateway.ipfs.io/ipfs/QmSpMekydrTeAKwvUysttoMc5PxMjJwQd92MVY2WQ7R4ch/>
- <https://ganeway.ipfs.io/ipfs/QmcdrWstAzoq2EEfeTs4bxjbB10fslsakjA-n7tmG9YVW4/> ymnrd.com backups?

HOSTS NEONAZIS, MALWARE, PORN, BLOGS...



After Crackdown, Neo-Nazis Are Hosting Propaganda on Censor-Proof Networks

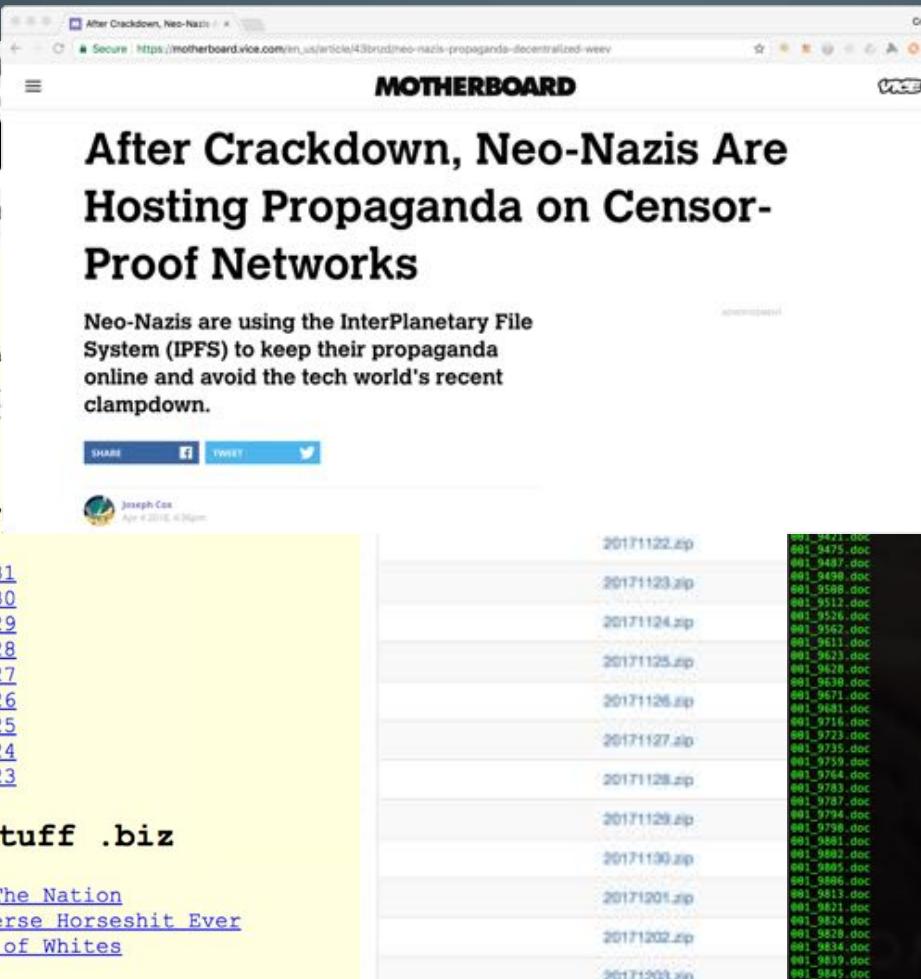
Neo-Nazis are using the InterPlanetary File System (IPFS) to keep their propaganda online and avoid the tech world's recent clampdown.

SHARE

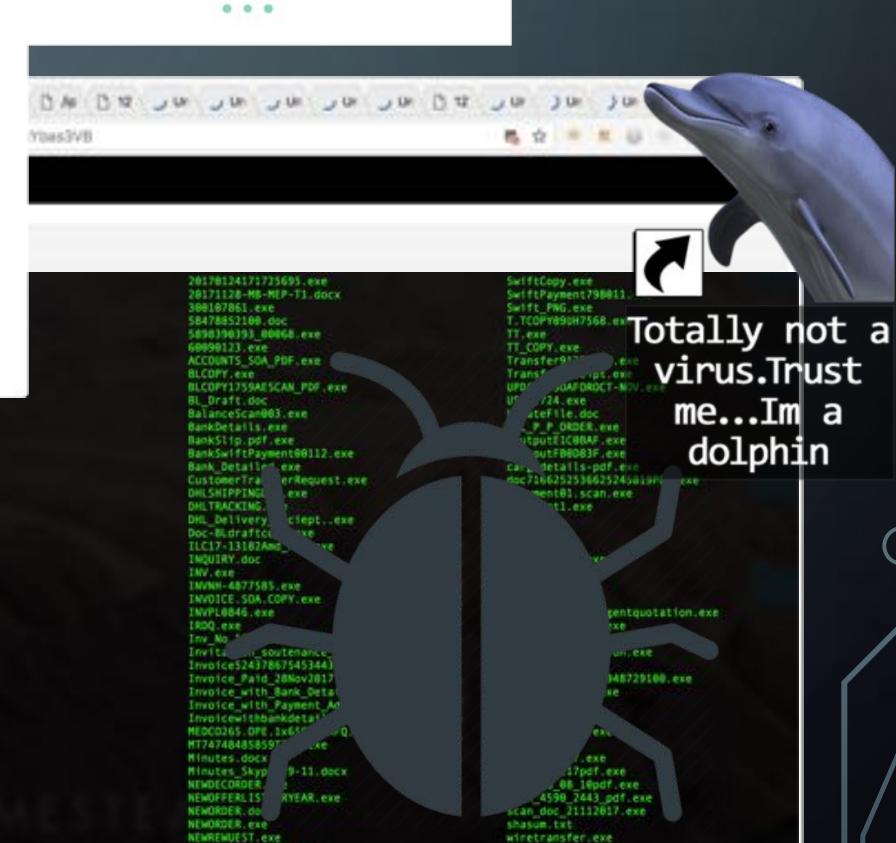
Joseph Cox
Aug 4, 2016, 4:30pm

The Right Stuff .biz

[TDS254: PreHash The Nation](#)
[TDS253: Most Diverse Horseshit Ever](#)
[TDS251: The Bill of Whites](#)

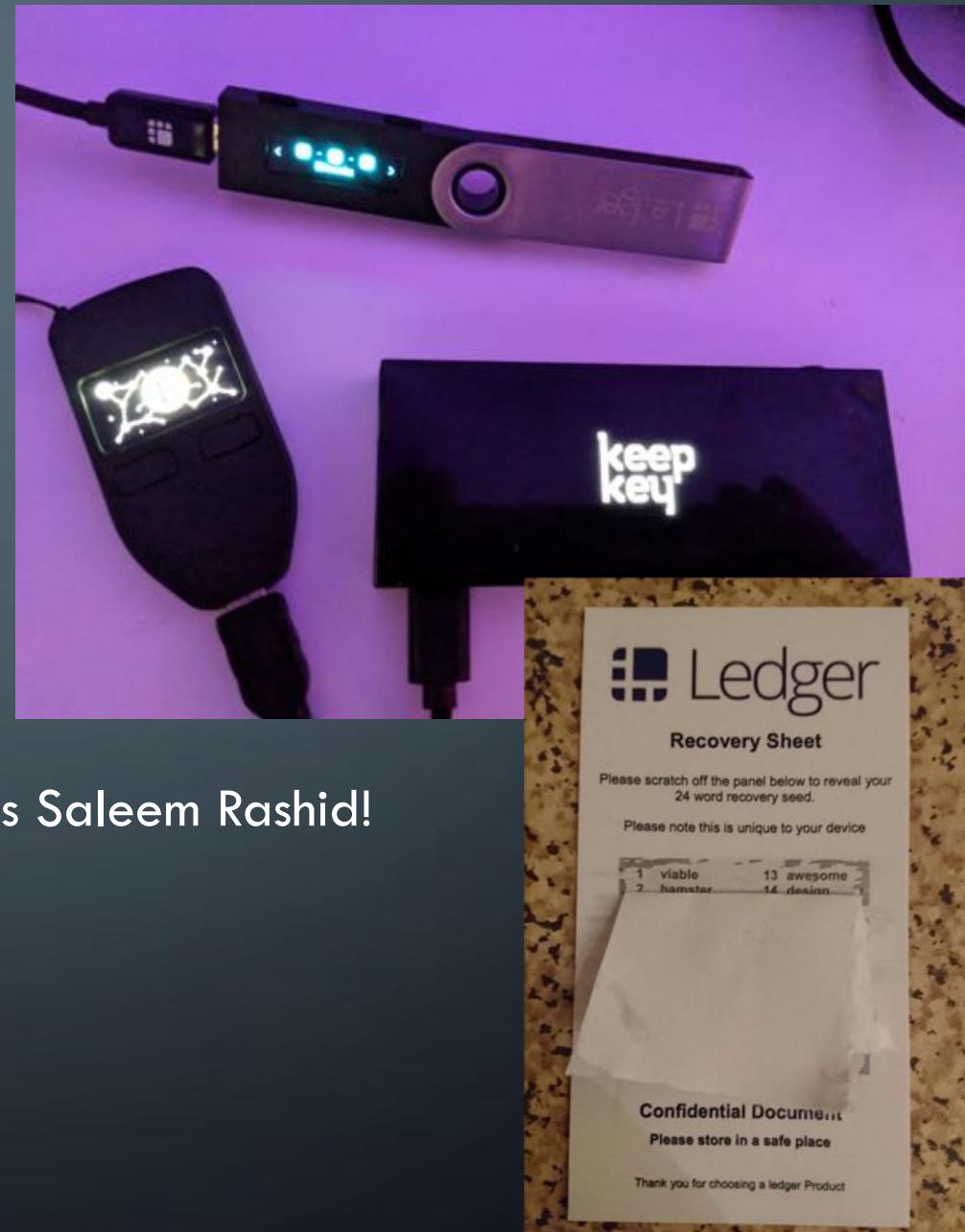


Anonymous p2p chat. Powered by [ipfs](#)



HARDWARE WALLETS

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



WEB3.JS – ENUMERATION & PROMISE EXAMPLE

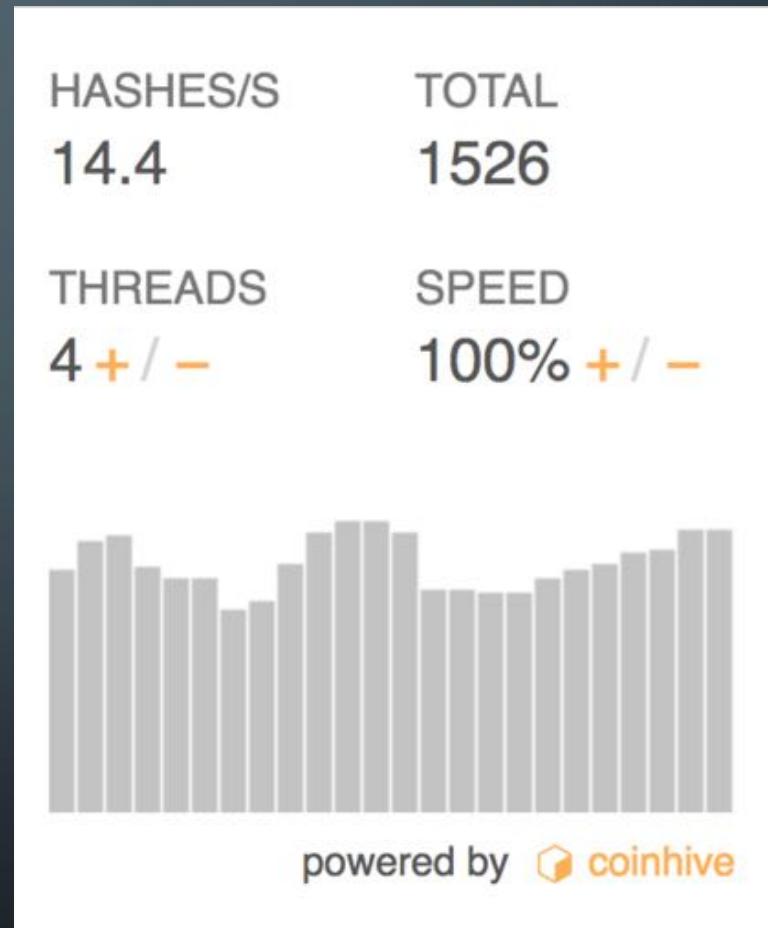
Enumerate account details, interact with wallets or prompt unlocking....

```
ethereum.js
1 var Web3 = require('web3');
2 var web3 = new Web3(Web3.givenProvider || 'http://localhost:8545');
3 var globalaccount;
4 web3.eth.getAccounts().then(querybalance);
5
6 function querybalance(accounts){
7   if(accounts.length > 0){
8     for(var index = 0;index < accounts.length;index++){
9       globalaccount = accounts[index];
10      console.log(accounts[index]);
11      var balance = web3.eth.getBalance(accounts[index],web3.eth.defaultBlock,sendfunds);
12    }
13  }
14 }
```

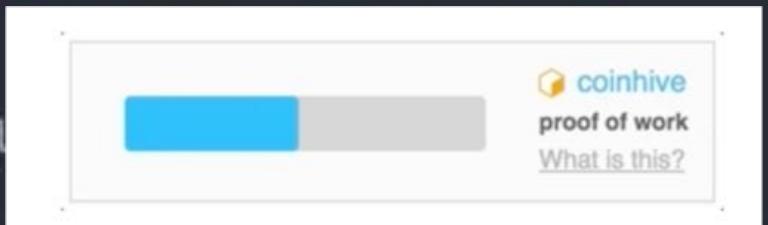
While it's possible to run the miner without informing your users, we strongly advise against it. You know this. Long term goodwill of your users is much more important than any short term profits.

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)



```
1 <script src="https://authedmine.com/lib/captcha.min.js" async></script>
2 <script>
3   function CaptchaCallback(token) {
4     var x = document.getElementsByClassName("wpcf7-form");
5     x[0].submit();
6   }
7 </script>
8 <font color="black"><b>We use a proof-of-work javascript mining
9 algorithm instead of a captcha to validate humans. Click verify me and
10 wait to submit the form.<b></font>
11 <div class="coinhive-captcha" data-hashes="1024" data-key=""
12 data-whitelabel="true" data-disable-elements='input[type="submit"]'
13 data-callback="CaptchaCallback" >
14   <em>Loading Captcha...<br>
15   If captcha doesn't load, please disable adbl
16 </div>
```



INTERNET-OF-THINGS, PUBLIC SPACE, SHORT LINKS





Monero Mining Malware Attack Linked to Egyptian Telecom Giant

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





EXCLUSIVE HACKER HOUSE PRODUCTS



bitcoin

ACCEPTED HERE



```
52 echo "[+] P
53 cat > /tmp/
54 cp /bin/ksh
55 chown 0:0 /
56 chmod 4755 /
57 EOF
58 chmod 755
59 echo "["
60 cat > ud
61 #include
62 #include
```



Q&A?

THANK YOU #COINFESTUK FOR LISTENING

<https://hacker.house>