Decentralizing Monero Mining

How and Why

Howard Chu

CTO, Symas Corp. hyc@symas.com

2022-06-18

Personal Intro

- Howard Chu
  - Founder and CTO Symas Corp.
  - Developing Free/Open Source software since 1980s
    - GNU compiler toolchain, e.g. "gmake -j", etc.
    - Many other projects...
    - I never use a software package without contributing to it
  - Worked for NASA/JPL, wrote software for Space Shuttle, etc.

Personal Intro

- Career Highlights
  - 2011- Author of LMDB, world's smallest, fastest, and most reliable embedded database engine
  - 1998- Main developer of OpenLDAP, world's most scalable distributed data store
  - 1995 Author of PC-Enterprise/Mac, world's fastest AppleTalk stack and Appleshare file server
  - 1993 Author of faster-than-realtime speech recognition using Motorola 68030
  - 1991 Inventor of parallel make support in GNU make

Personal Intro

- Security-related Highlights
  - 2015- Contributor to Monero
  - 2010- Maintainer of RTMPdump, reverse-engineering Adobe Flash encryption
  - 1996- Contributor to OpenSSL, including multi-precision math functions for Motorola 68020
  - 1995- Contributor to Kerberos
  - 1994- Discovered weakness in Andrew File Server's password hashing scheme
  - 1991 Co-inventor of TCPwrappers, used to secure internet server connections on Unix

Topics

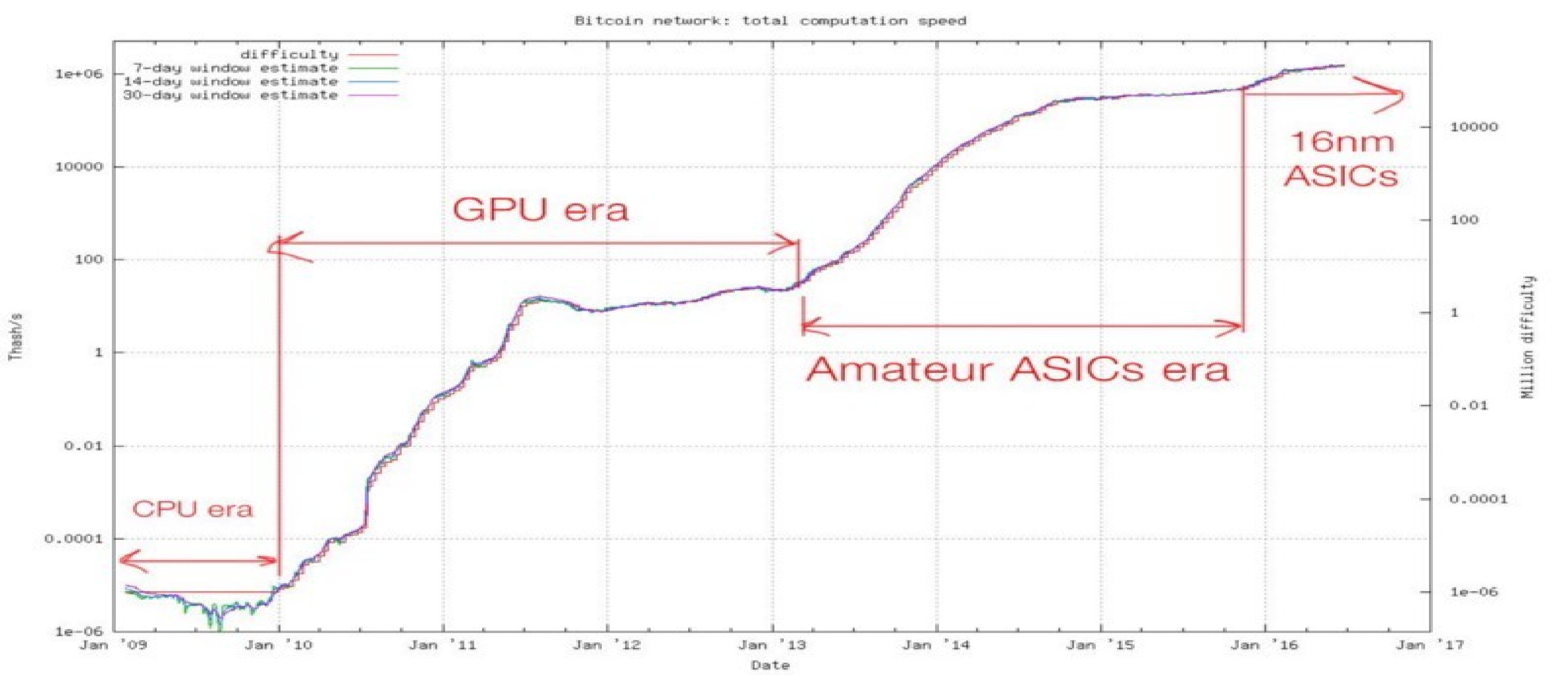
- What do we mean by Mining Decentralization?
  - Why is it important?
  - How do we achieve it?

Decentralization: Why?

- In the beginning…
  - Monero based on CryptoNote, designed ~2014
  - The CryptoNote design was a reaction to obvious flaws in the Bitcoin protocol/network/ecosystem
    - Pseudonymity inadequate for privacy and fungibility
    - Fixed parameters (e.g. blocksize) instead of dynamic
    - Heavy centralization, instead of promised decentralization

Decentralization: Why?

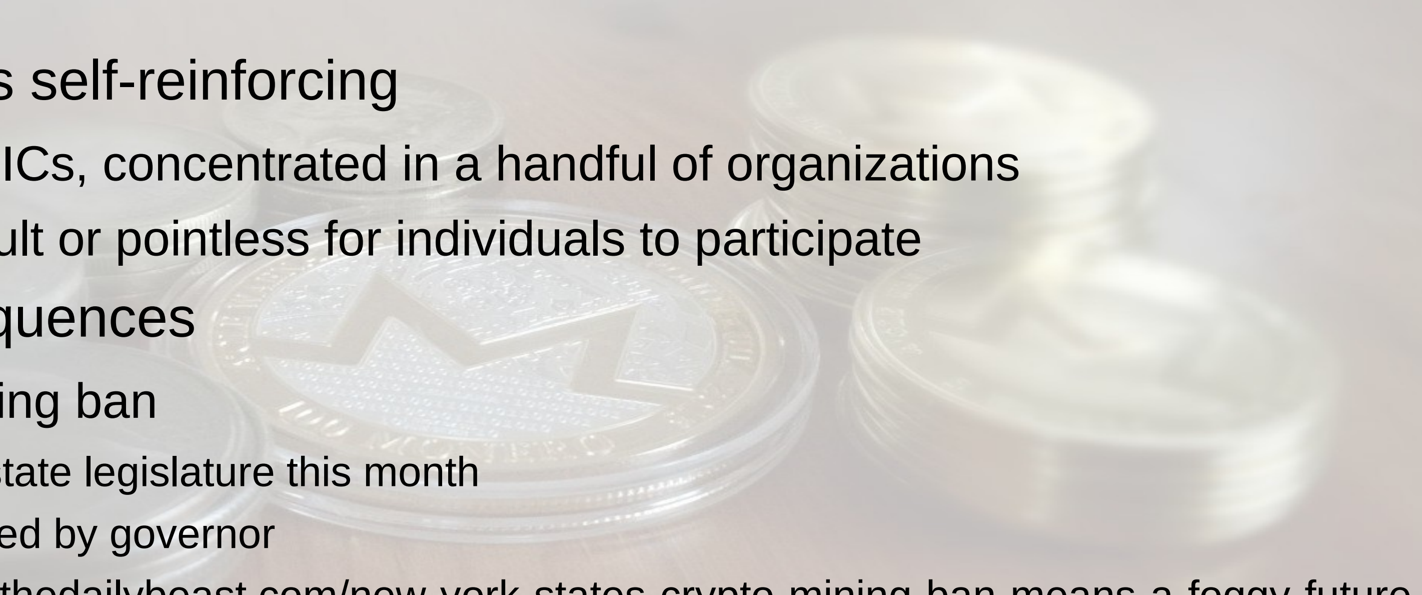
- Bitcoin mining hashrate trend



Decentralization: Why?

- In the beginning…
  - First Bitcoin mining ASIC from Avalon, February 2013
    - 50x performance advantage over CPUs
  - Modern ASICs are millions of times more efficient than CPUs
  - Specialized hardware promotes centralization
    - it’s never as widely available as commodity hardware
    - ASIC builders tend to keep their chips for self-mining, rather than selling to the general public

Decentralization: Why?



- Centralization is self-reinforcing
  - Scarcity of ASICs, concentrated in a handful of organizations
  - Makes it difficult or pointless for individuals to participate
- Real life consequences
  - New York mining ban
    - Passed by state legislature this month
    - Not yet signed by governor
    - https://www.thedailybeast.com/new-york-states-crypto-mining-ban-means-a-foggy-future-for-bitcoin-and-others
  - Chinese mining ban in 2021

Decentralization: Why?

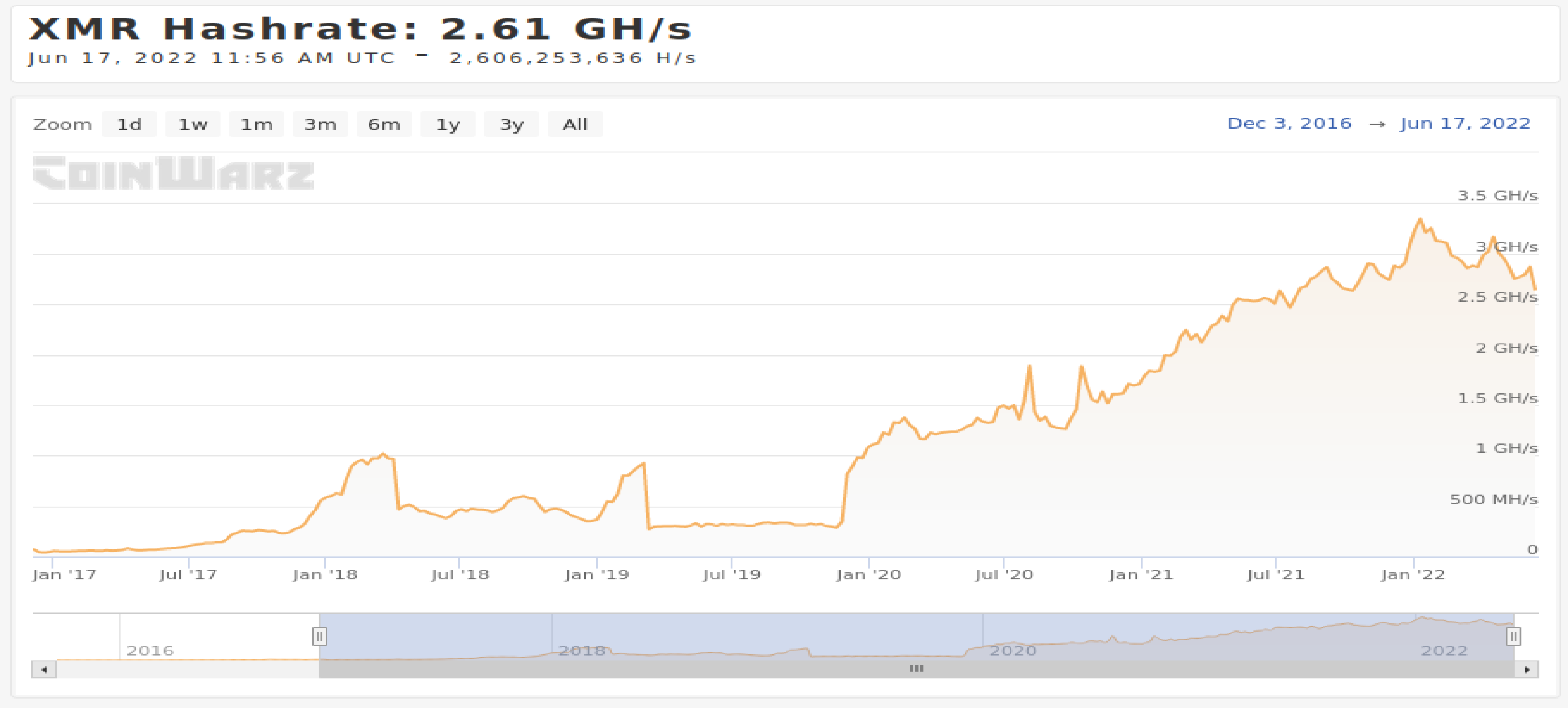
- … Chinese mining ban 2021
  - “hash rate dropped earlier this year, from April to July, as miners were forced by the CCP to leave China.”

Cryptocurrency	Hash Rate Change
Decred	-85%
Dash	-68%
Bitcoin	-63%
Litecoin	-56%
Zcash	-52%
Ethereum	-25%
Monero	+13%

Decentralization: How?

- Monero’s decentralization approach has been successful
- How are we achieving this?
  - ASIC Resistance via RandomX PoW algo
  - Pool decentralization via P2Pool

RandomX PoW



XMR Hashrate: 2.61 GH/s

Jun 17, 2022 11:56 AM UTC - 2,606,253,636 H/s

RandomX PoW

- General Approach
  - Use the task that CPUs are built for: running programs
  - Define our own virtual machine architecture and instruction set
  - Randomly generate code for this virtual CPU and execute it
  - Utilizes all the major components of a modern CPU

RandomX PoW

- Reasons for success/failure
  - PoW algos using fixed algorithms are all easily condensed into ASICs
  - The point of CPUs is not to run a single particular algorithm well, it’s to be able to run any arbitrary algorithm
  - Dynamically generating code is the only way to exercise this strength

RandomX PoW

- For more details, see the 2019 Monerokon presentation!

Algorithm	Instruction Fetch	Data Access	Floating Point	Syntax-Free
SHA256				
X11 / X16R				
CryptoNight		X		
Ethash		X		
Randprog/ RandomJS	X	X	X	
CryptoNight/R	X	X		X
ProgPow	X	X		
RandomX	X	X	X	X

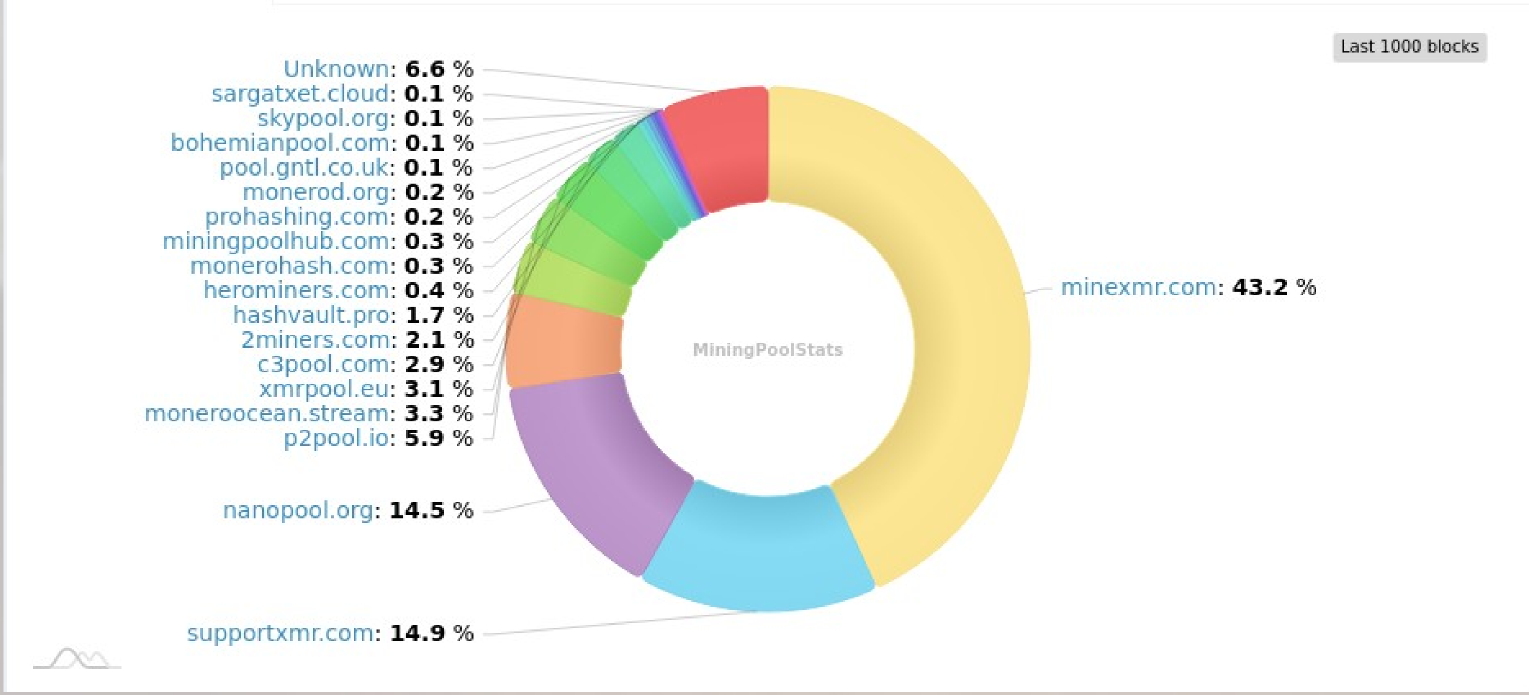
RandomX PoW

- Code Status
  - RandomX library
    - Full support for x86-64 and ARMv8: interpreter, AOT compiler, JIT
    - Interpreter support for everything else
  - Monerod
    - Fully integrated, mining and verification on mainnet since November 2019
  - GPUs are supported but not efficient

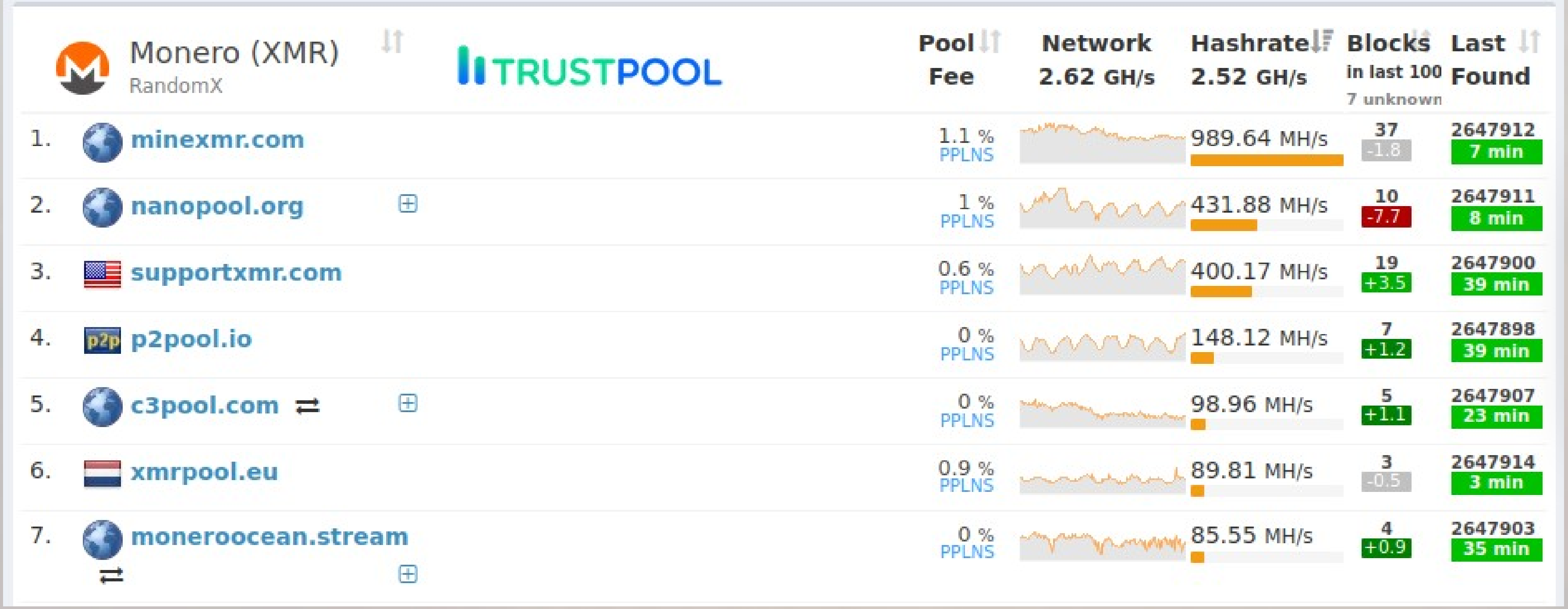
Misc Notes

- We know there were CryptoNight ASICs capable of mining CNv4 (CN/R) already in use, staying on CN variants was untenable
- Skeptics claimed RandomX would be defeated by ASICs within 6-12 months
- Today AMD Zen architecture is still best, but Apple M1/M2 is competitive
  - Too bad MacOS sucks
  - 5800X3D has little advantage, larger cache is slower

Pool Decentralization



Pool Decentralization



Monero (XMR)
RandomX

TRUSTPOOL

		Pool Fee	Network 2.62 GH/s	Hashrate 2.52 GH/s	Blocks in last 100 7 unknown	Last Found
1.	minexmr.com	1.1 % PPLNS		989.64 MH/s	37 -1.8	2647912 7 min
2.	nanopool.org	1 % PPLNS		431.88 MH/s	10 -7.7	2647911 8 min
3.	supportxmr.com	0.6 % PPLNS		400.17 MH/s	19 +3.5	2647900 39 min
4.	p2pool.io	0 % PPLNS		148.12 MH/s	7 +1.2	2647898 39 min
5.	c3pool.com ⇄	0 % PPLNS		98.96 MH/s	5 +1.1	2647907 23 min
6.	xmrpool.eu	0.9 % PPLNS		89.81 MH/s	3 -0.5	2647914 3 min
7.	moneroocean.stream ⇄	0 % PPLNS		85.55 MH/s	4 +0.9	2647903 35 min

What Is P2Pool?

- Originally developed for Bitcoin and abandoned
  - Merge mined sidechain with fast block rate
  - High frequency of orphan blocks
- Redeveloped by SChernykh from scratch
  - Adopts Uncle Blocks concept from Eth to fix orphan problem
  - 1st release Sep 2021

Mining Approaches

Pool type	Payouts	Fee	Min Payout	Centralized?	Stability	Control	Setup
Centralized pool	Regular	0-3%	0.001-0.01XMR	Yes	Subject to pool server outages	Pool admin controls funds, txn selection, can attack network	Only miner software is required
Solo	Rare	0%	0.6XMR	No	As stable as your Monero node	100% under your control	Monero node + optional miner
P2Pool	Regular	0%	~0.0003XMR	No	As stable as your Monero node	100% under your control	Monero node + P2Pool node + miner

P2Pool Details

- Fully decentralized, permissionless, and trustless
  - No pool admins, no central server
  - No pool wallet, payouts direct from blockchain
- Pay Per Last N Shares (PPLNS) payout scheme
  - PPLNS window of 2160 pool blocks (6 hours, 10sec blocks)
  - Payout proportional to total difficulty of shares in window

P2Pool Details

- Payouts direct via coinbase txn
  - Only supports primary addresses, not subaddresses
  - Coinbase txn addresses are public
    - Should use a separate wallet dedicated to P2Pool mining
- Advanced txn selection
  - Constructs blocks with better reward than monerod solo miner

P2Pool Details

- Supports arbitrarily many sidechains
  - Two are currently active, main and mini
  - Anyone can start a new sidechain
- Now available in Monero GUI v0.17.3.2
  - Easier for less techie users to participate

Questions?

References

1. https://medium.com/@lopp/the-future-of-bitcoin-mining-ac9c3dc39c60 Bitcoin mining stats 2013
2. https://www.researchgate.net/profile/Leonel_Sousa/publication/221291748_Improving_SHA-2_Hardware_Implementations/links/0912f50a8c7941c2b6000000/Improving-SHA-2-Hardware-Implementations.pdf
 SHA-2 block diagrams
3. https://en.bitcoin.it/wiki/CryptoNight CryptoNight overview
4. https://github.com/ethereum/wiki/wiki/Ethash Ethash specification
5. https://en.bitcoinwiki.org/wiki/X11 X11 overview
6. https://github.com/ethereum/wiki/wiki/Dagger-Hashimoto Random Circuit
7. https://github.com/hyc/randprog https://github.com/tevador/RandomJS RandomJS
8. https://github.com/ethereum/EIPs/blob/master/EIPS/eip-1057.md ProgPow
9. https://github.com/SChernykh/CryptonightR Cryptonight/R
10. https://www.prnewswire.com/news-releases/graphics-processing-unit-gpu-market-to-surpass-6761-million-by-2020-593938551.html GPU market stats
11. https://www.statista.com/statistics/272595/global-shipments-forecast-for-tablets-laptops-and-desktop-pcs/ PC market stats
12. https://www.statista.com/statistics/330695/number-of-smartphone-users-worldwide/ Smartphone market stats
13. https://github.com/tevador/RandomX RandomX

References

1. https://www.thedailybeast.com/new-york-states-crypto-mining-ban-means-a-foggy-future-for-bitcoin-and-others
   NY mining ban
2. https://medium.com/@tacorevenge/the-suppressor-part-2-on-chain-analysis-6561c5a478c4
   2021 hashrate
3. https://www.coinwarz.com/mining/monero/hashrate-chart Monero hashrate
4. https://miningpoolstats.stream/monero Monero pool stats
5. https://github.com/schernykh/p2pool P2Pool source
6. https://github.com/monero-project/monero-gui/releases/tag/v0.17.3.2 Monero GUI