On The Security and Ecological Sustainability of Monero

Francisco "ArticMine" Cabañas
articmine@getmonero.org

Konferenco
Lisbon, Portugal, April 19th, 2022

Proof of Work and Ecological Sustainability

Security Impacts 51% and Big Bang Revisited

Proof of Work (POW) Mining – Revisited Economic Assumptions

2008 Satoshi Nakamoto *Bitcoin: A Peer-to-Peer Electronic Cash System*
https://bitcoin.org/bitcoin.pdf

” ... The proof-of-work also solves the problem of determining representation in majority decision making. If the majority were based on one-IP-address-one-vote, it could be subverted by anyone able to allocate many IPs. Proof-of-work is essentially one-CPU-one-vote. The majority decision is represented by the longest chain, which has the greatest proof-of-work effort invested in it. If a majority of CPU power is controlled by honest nodes, the honest chain will grow the fastest and outpace any competing chains. ... “

What are the implicit economic assumptions is this statement?

Proof of Work (POW) Mining – Revisited Economic Assumptions

- Proof of work is performed. There are input costs, including electricity, equipment, real estate etc. There are also byproducts such as e-waste (obsolete equipment), heat, etc.
- The heat is equivalent in energy content to the electricity used. This is the first law of thermodynamics: **Energy can neither be created nor destroyed, only altered in form.**
- Object is a decentralized consensus.
- Honest miners are decentralized.
- Attacker is centralized.
- Proof of work has no marketable economic value, that could be sold, other than securing the network. Selling an economic value could favour the attacker.
- Security comes from the attacker having to match the time integrated electricity cost of the honest miners.
- What are the ecological externalizations? Do they favour the attacker? The honest miners?

Proof of Work (POW) Mining – Revisited Equipment

CPU vs GPU / Graphics Processors vs ASIC

- CPU most favourable to honest miners.
- Least ecological impact has many other users.
- Existing equipment can be repurposed for mining when not in use.
- Botnets can be mitigated and have to compete with other criminal activity.

- GPU / Graphics Processors favourable to honest miners.
- Have other uses.
- Have wide adoption: For example: Integrated graphics in mobile.
- Existing equipment can be repurposed for mining when not in use.

Proof of Work (POW) Mining – Revisited Equipment

CPU vs GPU vs ASIC

- ASIC least favourable to honest miners.
- Heaviest ecological impact.
- Centralized and proprietary production.
- Vertical Integration favours large industrial mining operations.
- Existing equipment can seldom if at all be repurposed for mining when not in use.
- Energy “efficiency” does not lower the mining energy consumption.
- Monero was attacked with ASICs in 2017 / 2018.
- Obsolete ASICs have little or no use after mining, except possibly as electric space heaters. They should not be used as boat anchors. This is to prevent Monero “boating accidents”.

Proof of Work (POW) Mining – Revisited Heat

- The input electricity gets converted entirely to heat.
- The value of heat produced is almost never zero contrary to the common assumptions.
- Example: Outside Temperature
  Madrid, Spain: On a hot summer day in July 40 C
  Edmonton, Canada: On a cold winter day in January -40 C
- Summer slight advantage to honest miners easier to dissipate heat that is distributed – Lower cooling cost – Still favours decentralization.
- Winter very heavy advantage to honest miners particularly for CPU Monero mining – Heavy advantage to decentralization
- Displacing electric space heating in many cases at zero cost in electricity or displacing natural gas with electricity.

Proof of Work (POW) Mining – Revisited Ecological Externalizations – Heat

Space Heating
Example: Sweden Space Heating
https://heatroadmap.eu/wp-content/uploads/2018/09/HRE4-Country_presentation-Sweden.pdf

- Very low cooling needs in summer.
- Highest energy demand in winter.
- 25% of residential space heating is electricity. Adding a CPU Monero miner has little or no impact on energy consumption of residence heated, provided it is small scale and decentralized.
- District Heating (Heat captured from thermal power generation etc.) 48% of residential space heating in mostly in multi family buildings.
- Major concerns over the energy impact of Bitcoin mining in the EU. The root cause: The Bitcoin miners were heating the outdoors in the winter with ASICs.
- Alternative: Heat the indoors, rather than the outdoors, in the winter by mining Monero with CPUs.

Proof of Work (POW) Mining – Revisited Ecological Externalizations – Heat

Space Heating
Example: British Columbia, Canada: Space Heating

- Natural Gas is cheap and plentiful: “Space heating accounts for between 67% and 84% of the total natural gas consumption for the buildings in this study. In British Columbia, space heating with natural gas represents the largest source of greenhouse gas (GHG) emissions from buildings.”
  https://www.endotherm.com/case-studies/bc-housing-research-energy-efficiency-impact-on-hydronic-heating-systems/
- Electricity Generation: 87% Hydro, 5% Biomass, 4% Wind, 4% Other
  https://www.cer-rec.gc.ca/en/data-analysis/energy-markets/provincial-territorial-energy-profiles/provincial-territorial-energy-profiles-british-columbia.html
- Little opportunity for district space heating.
- Electric heating is common in high rise residential.
- Impact of CPU Monero mining is either no impact or a subsidy to move away from Natural Gas to Electricity. Difference in cost between natural gas and electricity is mitigated by mining.
- Even adding a CPU Monero miner to an existing home heated with natural gas will lower CO_2 emissions.

Proof of Work (POW) Mining – Revisited Ecological Externalizations – Heat

Conclusions:

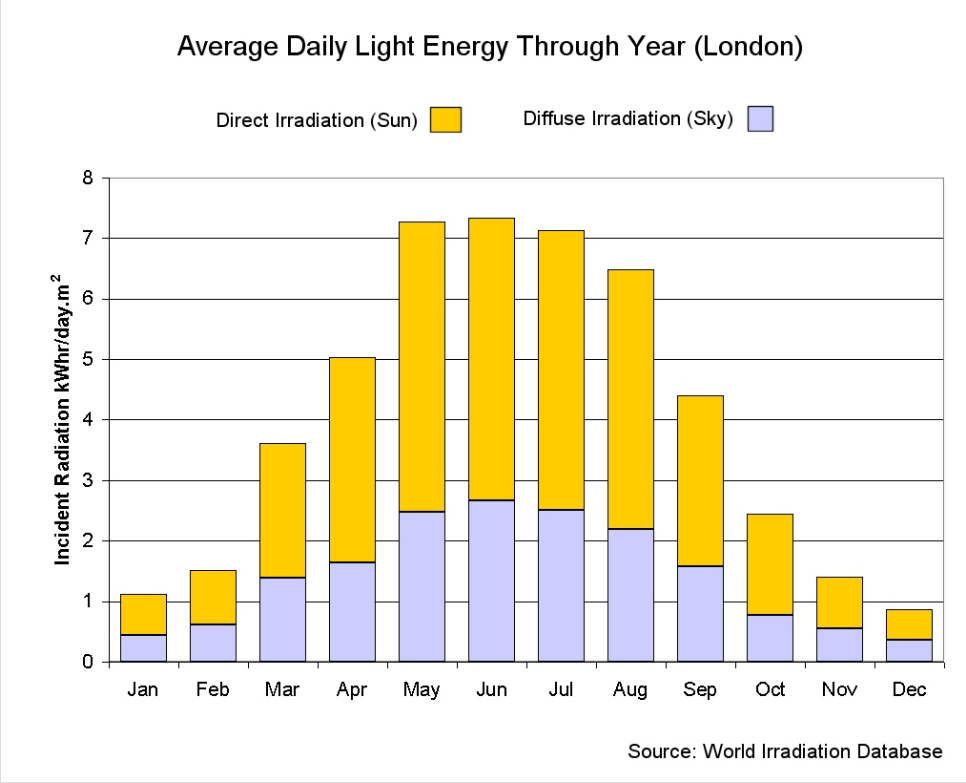
- Space heating using CPU Monero mining can have no impact on CO_2 emissions or even cause a reduction in CO_2 emissions.
- The lower effective cost to perform the POW by the honest miners leads to a higher POW hashrate at a given price. This leads to greater POW security by increasing the cost of a 51% attack
- The impact on the hashrate can be hard to quantify since cost savings / rebates from Monero mining have to have a significant impact overall on the heating cost.
- An extreme case there is little point in mining Bitcoin with CPUs or old ASICs even if the electricity is “free”.

Proof of Work (POW) Mining – Revisited Electricity Generation

Decentralized Examples:

- Diesel, Natural Gas, Petrol (Gas) Generators (Backup / On Demand)
  Solar Photovoltaic (PV)
  Wind, Small Scale Hydro.
- Centralized Examples:
  Nuclear (Thermal)
  Coal, Oil, and Natural Gas (Thermal)
  Natural Gas (Gas Turbine)
  Bio Fuel / Wood Waste (Thermal)
  Hydro, Tidal, Wind Farms, Solar (PV)
  Solar (Thermal).
- Thermal sources lend themselves to district heating.

Proof of Work (POW) Mining – Revisited
Solar (PV) Electricity Generation



Source:
https://www.viridiansolar.co.uk/resources-1-2-seasonal-variation-solar-energy.html

Proof of Work (POW) Mining – Revisited
Solar (PV) Electricity Generation

- Solar (PV) typically has a very significant seasonal variation peaking in the summer at mid latitudes.
- Maximizing solar output for a given amount of say roof space on a home or business means excess electricity in the summer.
- Selling it back to the grid may not be an option or a very low price is paid. If there are many sellers and one buyer the price will fall.
- Mining Monero with the excess power during the summer that would otherwise go to waste or be sold cheap becomes an option.
- Forced decentralization as there is a fixed amount of roof to mount solar panels.

Proof of Work (POW) Mining – Revisited

- POW mining can be made to work in a sustainable way, provided it is truly decentralized. This means 1 CPU 1 vote or theoretically 1 ASIC 1 vote.
- Decentralization is critical to take advantage of low miner density for space heating displacement and the use of low value excess solar PV electricity.
- Small business or home based mining operations that consume less electricity that is needed for their own space heating or have excess solar PV power can be CO_2 neutral or even lower CO_2 emissions.
- Regulation needs to focus on large centralized industrial mining operations, especially on those who heat the outdoors during winter, and encourage or at least not impact small scale mining in homes and small businesses.
- The above approach to regulation is beneficial to the crypto currency networks and may even allow for 1 ASIC 1 vote.

Proof of Work (POW) Mining – Revisited Security and Privacy Implications for Monero

- The increased usage of Monero mining for space heating and the use of excess solar solar PV electricity for Monero mining will increase the cost of a 51% attack in Monero
- One manifestation of this is the anecdotal observation that:
  ”It is not cost effective to mine Monero”
- Quantifying the by how much the cost of a 51% attack will increase above the nominal assumption of 0.3 XMR (1/2 the block reward) per block will require additional research.
- Attacks such as Big Bang are of course not affected, while the ratio of Big Bang to 51% will be affected.

The Monero Fee Market

- The problem of a miner adding transaction to a block is Monero is a discrete optimization problem.
- One can make an approximation to the discrete optimization problem, the infinitesimal transaction approximation, as follows:
- The miner orders the transactions in order of fee paid per byte.
- The miner then adds transactions to the block starting with the highest paying transactions first.
- The miner then tests after each transaction for profit.
- The miner then stops when either the additional penalty for adding a transaction is greater than transaction fee, there are no more transactions, or the maximum blocksize (double the short term median) is reached.

The Monero Fee Market

- Define Block Size = (1+B) M_L where M_L is the short term median
- We add a transaction of size T_T to a block at a point B in the penalty, and define $B_T = T_T / M_L$; the new penalty becomes $R_{base}(B+B_T)^2$. The difference between the old and the new penalty is then $R_{base}(2BB_T + B_T^2)$
- The fee paid by the last included transaction must cover any additional penalty or $F_T = R_{base}(2BB_T + B_T^2)$.
- This is the lowest fee per byte paid in the block.
- For B = 1 and $B_T << 1$ one gets a minimum of $4R_{base}$
- The penalty gets R_{base} Honest miners make a profit of $3R_{base}$
- This assumes a free market interaction between rational miners and users.

Pricing Big Bang – Revisited

- The Big Bang attack[1] proposed an attacker will spam the Monero network to double every 100 blocks and attributed the cost of the attack to the block reward per block, R_{base}.
- This analysis does not take into account the impact of the long term median introduced in 2019.
- This was based upon my post in BitcoinTalk where I mentioned the lower bound was at least the block reward R_{base}[2].
- The BitcoinTalk post did not take into account the game theory of the Monero Fee Market.
- If the Monero Fee Market is taken into account the cost of Big Bang per block is $4R_{base}$ with R_{base} going to the penalty and $3R_{base}$ going to the honest miners.
- If the attacker already has 51% then the additional cost is R_{base}

1) https://github.com/noncesense-research-lab/Blockchain_big_bang/blob/master/models/Isthmus_Bx_big_bang_model.ipynb

2) https://bitcointalk.org/index.php?topic=753252.msg13591241#msg13591241

Final Thoughts

- Monero mining becomes sustainable by using electricity that would have been used for space heating or from surplus solar PV that would otherwise had gone to waste or has very low value.
- This has a direct impact of increasing the cost of a 51% attack above the nominal 0.3 XMR (1/2 of the block reward). Quantifying this requires further research.
- The Big Bang attack is at least 2.4 XMR per block, before factoring in the long term median.

Questions and Discussion