Minting Money With Megawatts

How to mine Bitcoin profitably

Sveinn Valfells, PhD[1] & Jón Helgi Egilsson[2]

[1]linkd.in/wtaHi5

[2]Faculty of Economics
University of Iceland

Presented at Scaling Bitcoin, Montreal
September 13, 2015

Outline

Outline

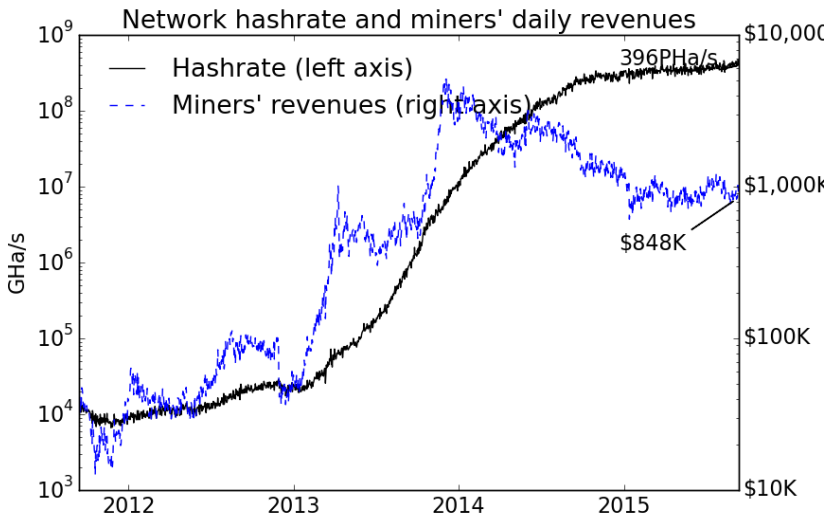
Mining Defines The Character of Bitcoin

Computational proof secures the Bitcoin blockchain [1]

"The solution we propose begins with a timestamp server."

— Satoshi Nakamoto [1]

- Low-trust solution to double spending problem.
- Miners' "proof of work" clears and secures transactions.
- New services may expand market.
- Financial and technological barriers to entry.
- Consolidation may erode "trustless, decentralized" character of Bitcoin.



- Trailing 365 day mining revenues: $386M.

Miners Compete For Network Share

Costs determined by system specifications and deployment environment

$$\pi(X) = \frac{X}{h_0 + X} \times B \times (S + F) - X \times C - \frac{1}{T} \times \left(\frac{X}{z} + NRE \right) \quad (1)$$

X Incremental hashing capacity.

B Bitcoin price.

S New supply.

F Transaction fees.

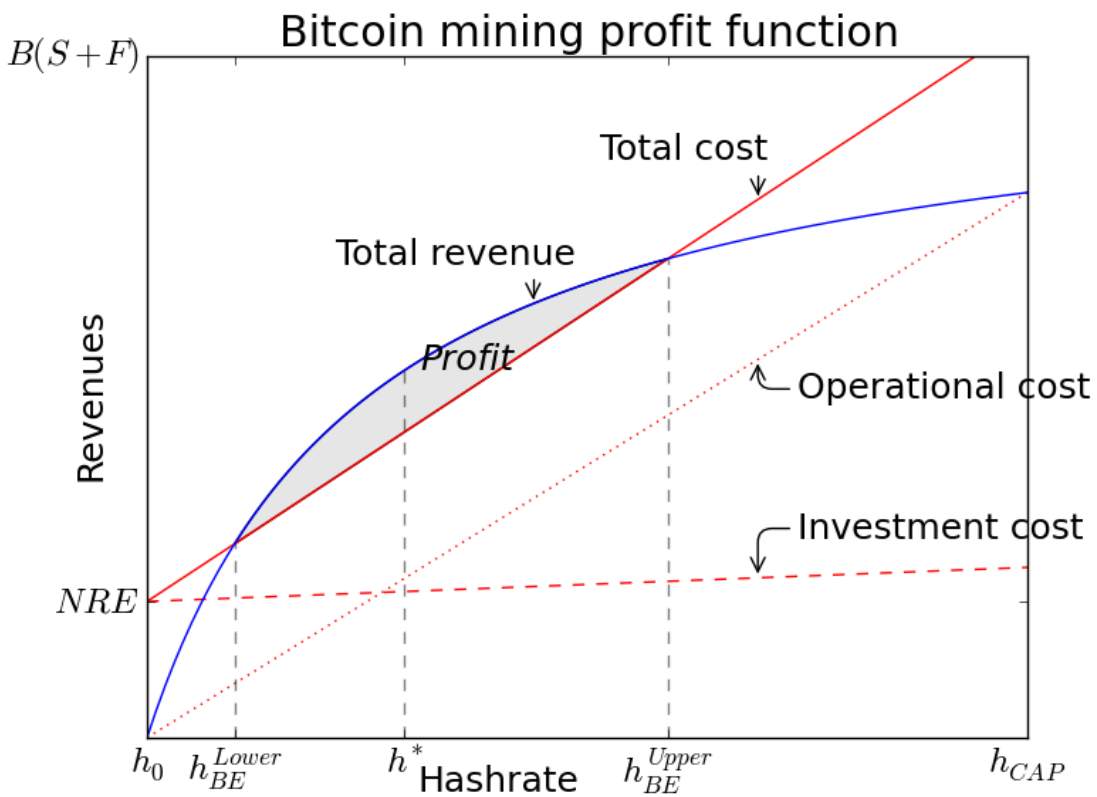
h_0 Initial hashing capacity.

C Operational costs.

z Technological factor of production.

NRE Non-Recurring Engineering costs.

T Amortisation period.



Profit Function Determines Network Size

Key points depend on technology and investment time horizon

Maximum hashrate

$$h_{CAP} = \frac{B(S+F)}{C} \tag{2}$$

Hashrate of maximum profitability

$$h^* = \sqrt{\frac{h_0 B(S+F)}{C + \frac{1}{zT}}} \tag{3}$$

Breakeven hashrate

$$h_{BE}^{Upper/Lower} = h_0 + \frac{(B(S+F) - h_0(C + \frac{1}{zT}) - \frac{NRE}{T})}{2(C + \frac{1}{zT})} \pm \frac{\sqrt{(B(S+F) - h_0(C + \frac{1}{zT}) - \frac{NRE}{T})^2 - 4(C + \frac{1}{zT})h_0 \frac{NRE}{T}}}{2(C + \frac{1}{zT})} \tag{4}$$

Implied amortisation $T_{Implied}$

Calculate shortest profitable payback period or implied amortisation, $T_{Implied}$ (using Equation 4).

Moore's Law Is Key Efficiency Driver

Semiconductor technology will improve efficiency in near and medium term

C Operational cost ($).

CLC Co-location and power cost ($).

POW ASIC energy efficiency ($/PHa/s).

PUE Datacentre energy efficiency (> 1).

UTZ Equipment utilisation (< 1).

$$C = \frac{CLC \times POW \times PUE}{UTZ} \tag{5}$$

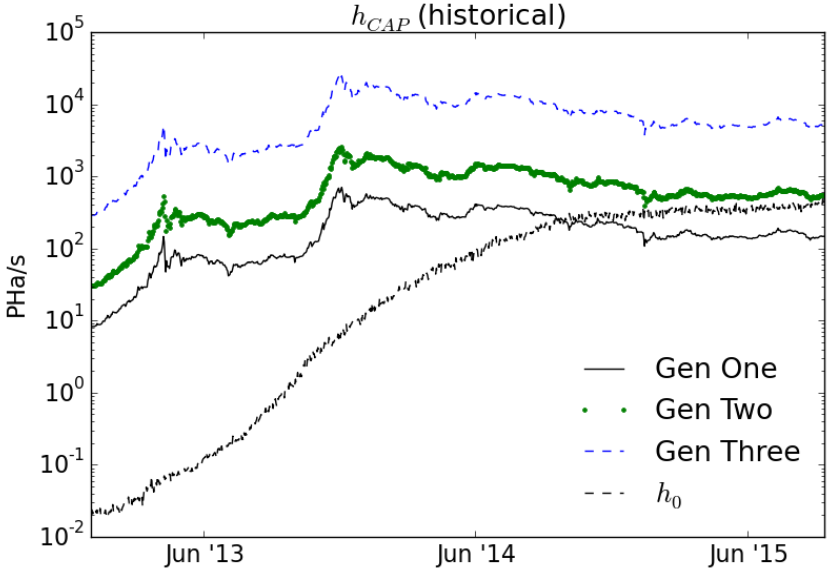
	CLC $/kW/month	NRE $	INV $/PHa/s	POW W/GHa/s	PUE None	UTZ None
Generation One	150	2M	10M	0.8	1.2	0.8
Generation Two	100	4M	1M	0.4	1.1	0.9
Generation Three	50	8M	0.5M	0.1	1.03	0.99999

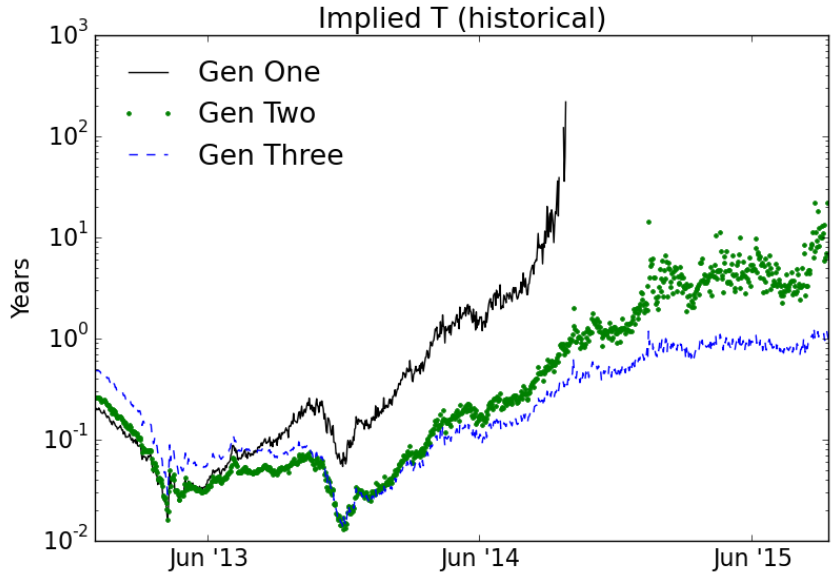
Table : Characteristic price and performance numbers for three generations of Bitcoin mining ASICs and their deployment environments [2, 3].

Network Approaching State Of Current Art

First and second generations outdated at $240 and 396 PHa/s [4]

g





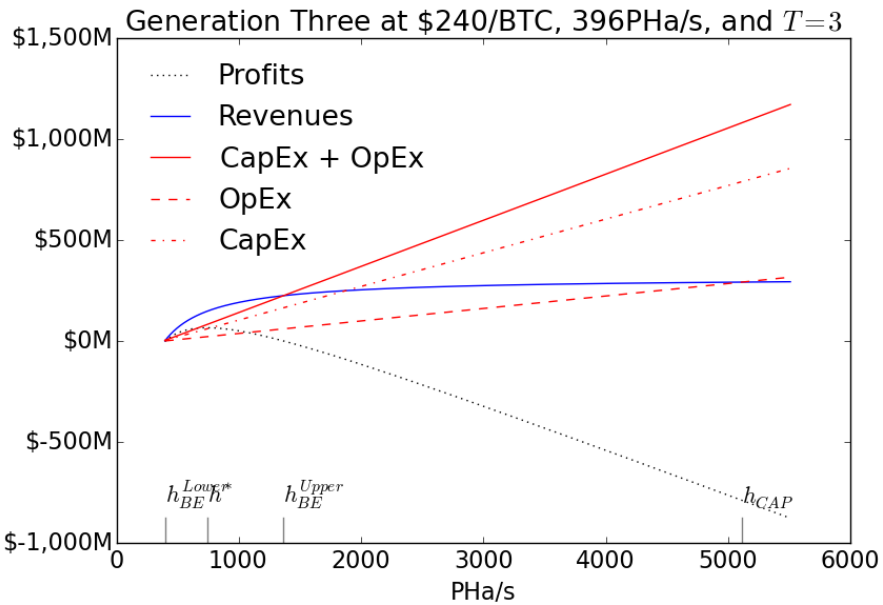
- Gen One no longer profitable.
- Gen Two close to economic limit.

- Gen Three has short payback $T_{Implied}$.
- Price volatility influences T_{Market}.

Network Has Room For Growth

Generation Three can double network size at current price

$T = 0.5$	h_{BE}^{Lower} PHa/s	h_{BE}^{Upper} PHa/s	h^* PHa/s	h_{CAP} PHa/s	Margin %
Generation One	nan	nan	nan	146	-172
Generation Two	nan	nan	nan	539	26
Generation Three	nan	nan	nan	5115	92
$T = 1$					
Generation One	nan	nan	nan	146	-172
Generation Two	nan	nan	nan	539	26
Generation Three	461	484	472	5115	92
$T = 3$					
Generation One	nan	nan	nan	146	-172
Generation Two	nan	nan	nan	539	26
Generation Three	401	1367	741	5115	92
$T = 5$					
Generation One	nan	nan	nan	146	-172
Generation Two	nan	nan	nan	539	26
Generation Three	399	1941	880	5115	92



- Generation Three is "State of the Art".
- Maximum processor power efficiency doubles every three years [5].

`https://github.com/sweyn/bitcoin-mining-profitability`

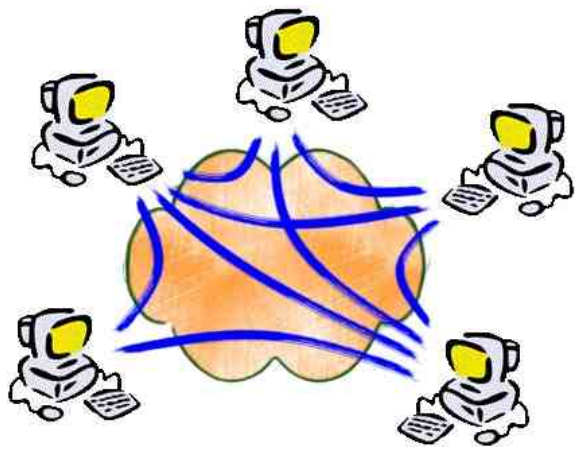
New Strategies Could Change The Game

New technologies or new deployment strategies could disrupt mining

"[W]here no player has an incentive to deviate from his or her chosen strategy after considering an opponent's choice."

— Nash Equilibrium [6]

- Amortize *NRE* over large batch.
- Push down variable investment cost with large volumes.
- Minimize system energy dissipation.
- Allow discovery of low electricity prices.
- Up to ≈10 GHa/s feasible on smartphones (10^5 phones for 1 PHa/s)



$$\pi(X) = \frac{X}{h_0 + X} \times B \times (S + F) - X \times \frac{CLC \times POW \times PUE}{UTZ} - \frac{1}{T} \times \left(\frac{X}{z} + NRE \right)$$

Mining Has Room Profitable Growth

Mining will scale with Bitcoin, network will grow and become more efficient

Network size Mining network supports growth up to $\approx 1300\,\mathrm{PHa/s}$.

Efficiency Efficiency can improve substantially while Moore's Law is valid.

Dynamics Miners will compete on technology, operational efficiency, deployment strategy, and cost of capital.

Endstate Window to entry has narrowed, market will consolidate.

Revenues Revenues will shift from new issue to transfer fees.

Key factors Expectations of Bitcoin price and volatility will determine level of investment (T_{Market} versus $T_{Implied}$).

Surprises New applications (merged mining); new processor platforms (graphene); new deployment strategies (embedded mining).

Conclusion Bitcoin is a compelling innovation which is likely to scale.

Outline

Some Relevant Previous Remarks

Bitcoin is potential dynamite waiting to be ignited.

— Communication with Teddy Shalon, August, 2011

Bitcoin can easily be projected to rise to $20 – $120 within three years.

— Communication with Pamir Gelenbe, January, 2013

We expect Bitcoin mining revenues to grow to $600M within three years . . . network capacity will rise 50–300×. The total energy requirement will be at least 12 MW and possibly as much as 70 MW.

— Memorandum to Landsvirkjun, August, 2013 [7]

I encourage people to do their own research and only risk as much as they are willing to lose in Bitcoin or any other virtual currency.

— BBC Newsnight, November, 2013

MtGox failure is not systemic . . . trend of Bitcoin will continue upwards but will be interspersed with price spikes and corrections.

— BBC World News & BBC World Business Edition, February, 2014

References

[1] Satoshi Nakamoto. Bitcoin: A Peer-to-Peer Electronic Cash System. http://bitcoin.org. May 24, 2009.

[2] The Bitcoin Wiki. Mining hardware comparision. `https://en.bitcoin.it`. Retrieved, August, 2013.

[3] Nermin Hajdarbegovic. Kncminer plans 16nm bitcoin mining asic launch in 2015. CoinDesk. November 18, 2014.

[4] Blockchain.info. Bitcoin Block Explorer. `https://blockchain.info`. Retrieved, April 17, 2015.

[5] Jonathan Koomey & Samuel Naffziger. Moore's Law Might Be Slowing Down, But Not Energ Efficiency. IEEE Spectrum. March 31, 2015.

[6] Investopedia. Nash equilibrium. `http://www.investopedia.com`. Retrieved, September 2015.

[7] Jón H Egilsson & Sveinn Valfells. Global Payment Processing Using Icelandic Energy Resources. Memorandum for Landsvirkjun. August, 2013.

Outline

Bigger Blocks Are Better For Bitcoin

1Mb limit is artificial constraint which must be expanded, question is when and how

Block size Mb	Max yearly data Gb	Max growth rate Mbps
1Mb	53	0.013
8Mb	420	0.110

Table : Change in blockchain data requirements with increase in blocksize from 1Mb to 8Mb.

Compare with retail smartphone:

- iPhone6+ storage up to 128Gb.
- iPhone6+ bandwidth up to 168/22Mbps.