How to Mine Bitcoin Profitably

Minting Money With Megawatts

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

[1] linkd.in/wtaHi5

[2] Faculty of Economics
University of Iceland

Presented at The Icelandic Computer Society

November 18, 2015

Outline

1. Bitcoin Mining: A Network of Distributed Timestamp Servers
2. How to Mine Bitcoin Profitably
3. About the Authors

Outline

1. Bitcoin Mining: A Network of Distributed Timestamp Servers
2. How to Mine Bitcoin Profitably
3. About the Authors

Bitcoin Is A Platform For Storing And Transmitting Value

Bitcoins are tokens for transacting on a distributed ledger, the blockchain [1, 2, 3]

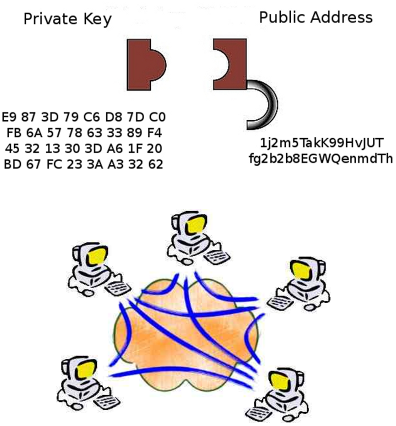


Figure : Private–public key public used for authentication (top); transactions broadcast on a peer-to-peer network (bottom).

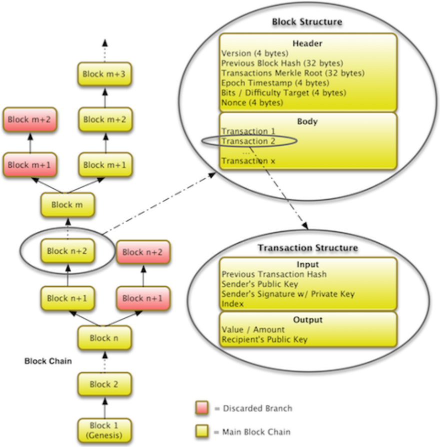


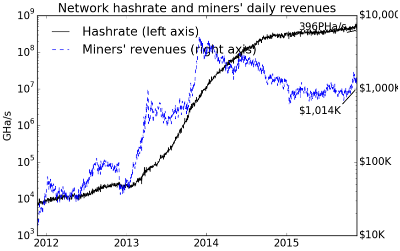
Figure : New transactions timestamped with SHA256 hash every 10m.

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: $358M.

Hashes Protect The Integrity Of The Blockchain

Miners search for SHA256 hashes of new block headers [4]

SHA256 example: The quick brown fox jumps over the lazy dog[.]

c03905fcdab297513a620ec81ed46ca44ddb62d41cbbd83eb4a5a3592be26a69

b47cc0f104b62d4c7c30bcd68fd8e67613e287dc4ad8c310ef10cbadea9c4380

Blockchain hashing:

Field	Purpose	Updated when...	Size (Bytes)
Version	Block version number	New protocol version	4
hashPrevBlock	256-bit hash of the previous block header	A new block comes in	32
hashMerkleRoot	256-bit hash based on all of the transactions in the block	A transaction is accepted	32
Time	Current timestamp as seconds since 1970-01-01T00:00 UTC	Every few seconds	4
Bits	Current target in compact format	The difficulty is adjusted	4
Nonce	32-bit number (starts at 0)	A hash is tried (increments)	4

Block 345,981: 000000000000000003e560d227c225b5cdf7bcee3358d53222d5d0af6240db4d

Outline

1. Bitcoin Mining: A Network of Distributed Timestamp Servers

2. How to Mine Bitcoin Profitably

3. About the Authors

Miners Compete For Network Share

Costs determined by system specifications and deployment environment

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

X Incremental hashing capacity.

B Bitcoin price.

S New supply.

F Transaction fees.

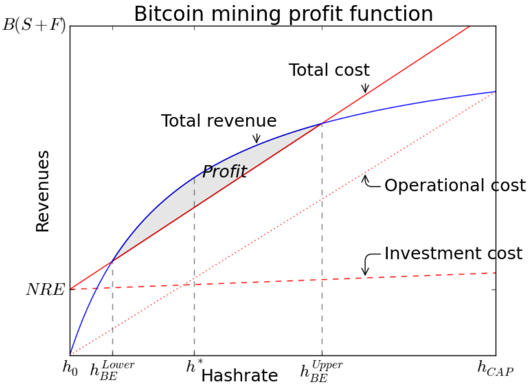
h_0 Initial hashing capacity.

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

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

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

$$\pi(X) = \frac{X}{h_0 + X} \times B \times (S + F) \times UTZ - X \times CLC \times POW \times PUE - \frac{1}{T} \times (X \times INV + NRE) \tag{5}$$

CLC Co-location and power cost ($).

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

PUE Datacentre energy efficiency (> 1).

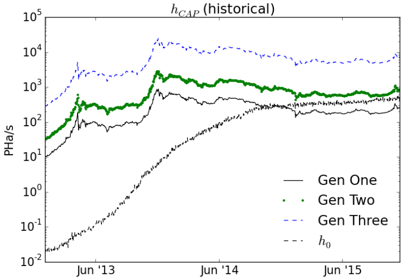
UTZ Equipment utilisation (< 1).

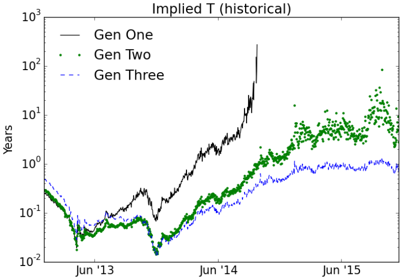
	CLC	NRE	INV	POW	PUE	UTZ
	$/kW/month	$	$/PHa/s	W/GHa/s	None	None
Generation One	150	2M	10M	0.8	1.2	0.8
Generation Two	100	4M	1M	0.4	1.1	0.9
Generation Three	50	8M	0.5M	0.1	1.03	0.99999

Table : Characteristic price and performance numbers for three generations of Bitcoin mining ASICs and their deployment environments [5, 6].

Network Approaching State Of Current Art

First and second generations outdated at $332 and 396 PHa/s [7]





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

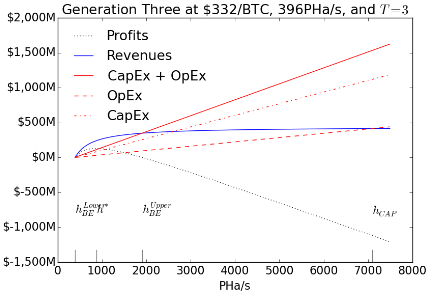
- Gen Three has short payback $T_{Implied}$.
- Price volatility influences T_{Market}.

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	254	-96
Generation Two	nan	nan	nan	831	47
Generation Three	nan	nan	nan	7096	94
$T = 1$					
Generation One	nan	nan	nan	254	-96
Generation Two	nan	nan	nan	831	47
Generation Three	412	750	556	7096	94
$T = 3$					
Generation One	nan	nan	nan	254	-96
Generation Two	409	444	449	831	47
Generation Three	399	1905	872	7096	94
$T = 5$					
Generation One	nan	nan	nan	254	-96
Generation Two	399	538	488	831	47
Generation Three	398	2699	1036	7096	94

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



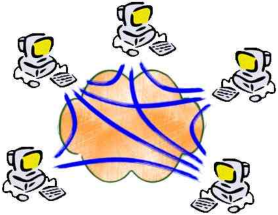
- Generation Three is "State of the Art", entry price $\gtrsim$\$10M.
- Maximum processor power efficiency doubles every three years [8].

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 [9]

- 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)



Mining Has Room For Profitable Growth

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

Network size Mining network supports growth up to $\approx 1900\,\mathrm{PHa/s}$.

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

1 Bitcoin Mining: A Network of Distributed Timestamp Servers

2 How to Mine Bitcoin Profitably

3 About the Authors

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 [10]

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] Wikipedia. Bitcoin. http://en.wikipedia.org. Retrieved April, 2015.

[3] Dirk Merkel. Bitcoin for beginners, Part 2. http://www.javaworld.com. December 6, 2011.

[4] Wikipedia. SHA-2. http://en.wikipedia.org. Retrieved February, 2015.

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

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

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

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

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

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