SWINBURNE UNIVERSITY OF TECHNOLOGY

Theory of Blockchain

Session 12:

Economics of Blockchain

Module 3 – Economics of Mining

Blockchain <-> Mining: a love-hate relationship

- Some blockchains (mostly PoW-based ones) created the mining industry (e.g. Bitcoin).

- Some tried to mitigate the side effects and lower the cost of consensus by adopting algorithms different from PoW (e.g. Ethereum 2.0’s PoS mechanism)

- Some blockchains tried to completely avoid mining by not relying on very hard work to reach consensus (e.g. DAG-based IOTA).

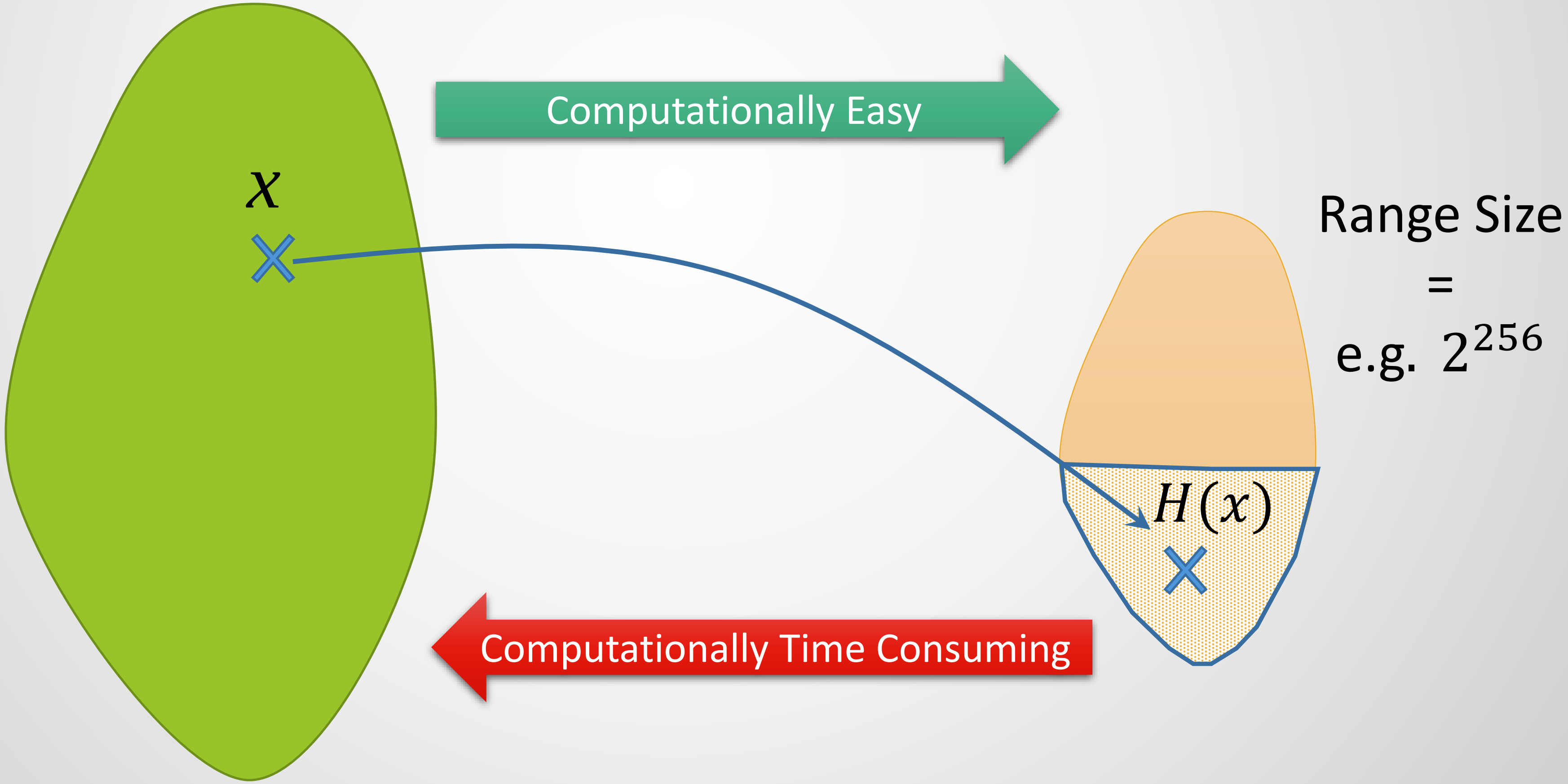
Mining Concept

- Mining by PoW usually means proving that you have solved a hard mathematical problem or puzzle.

- The puzzle is normally designed to be solvable only by trial and error.
  - In the case of Bitcoin, the problem is finding a hash value smaller than a threshold.
  - It is done by changing a nonce (in the header) and hashing multiple times to get a result.

Do You Recall Bitcoin PoW Puzzle?

Instead of finding a point like x that exactly maps to H(x), we want to find a point like x that maps to any point inside a region in the range.



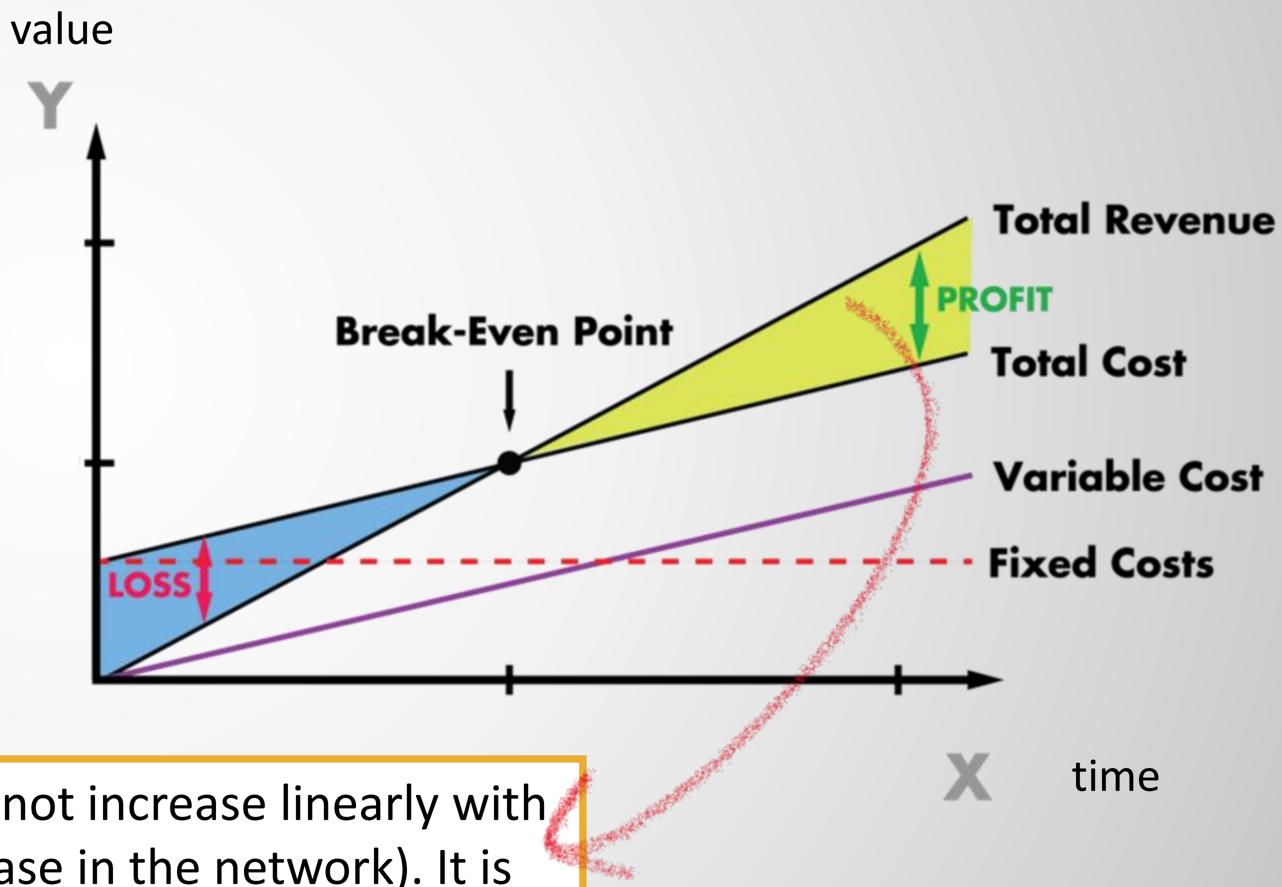
Mining Profitability

Cost = Cost of Hardware (fixed)

+ Cost of Energy

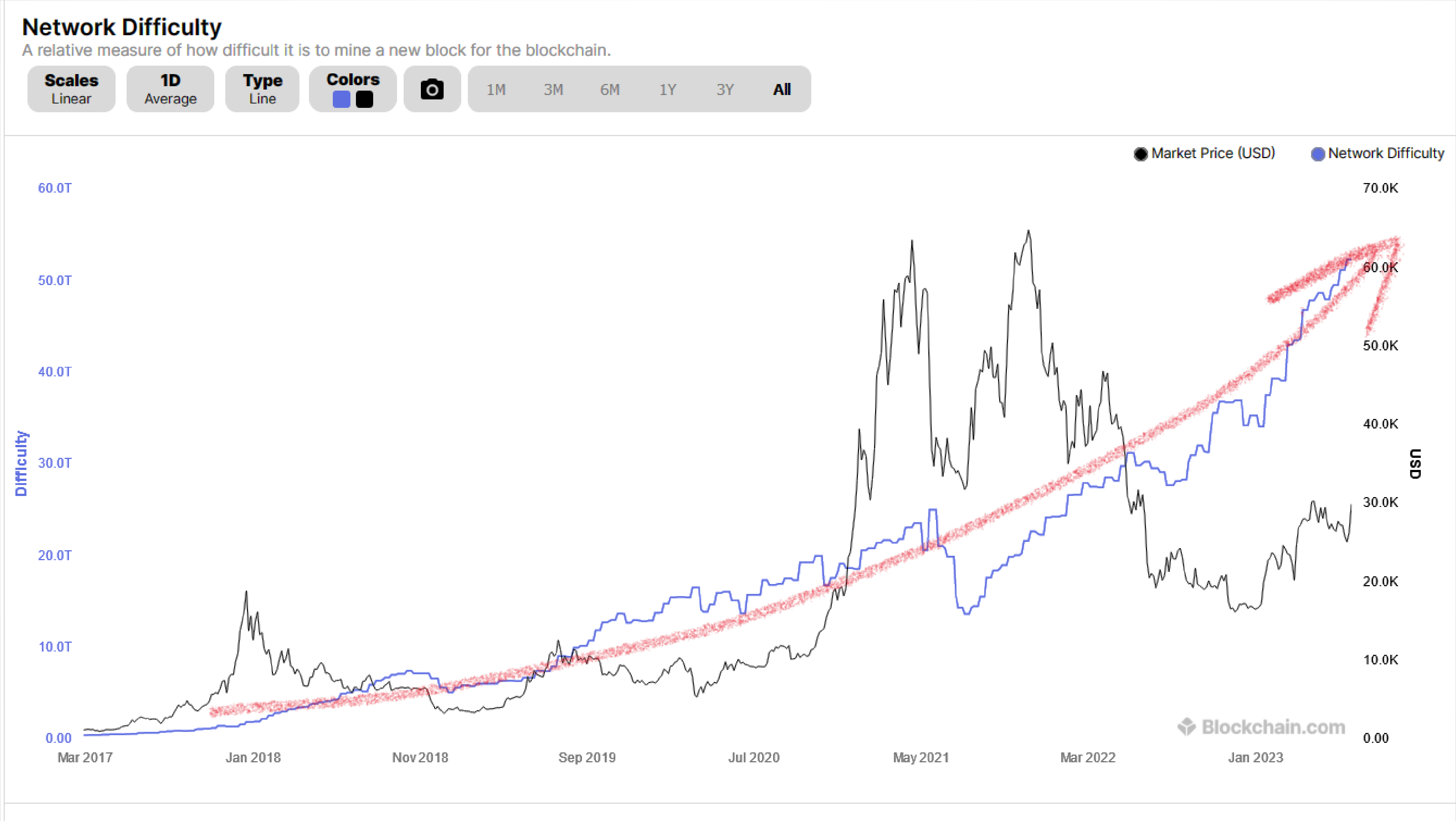
+ Other Costs

- Other costs could be warehouse rent, repair/maintenance, wages, etc.



The issue is that this revenue does not increase linearly with time (mainly due to difficulty increase in the network). It is normally bent since the hardware computational power is fixed but the puzzle hardship grows with time.

BTC Puzzle Difficulty (+ BTC Price)



Network Difficulty

A relative measure of how difficult it is to mine a new block for the blockchain.

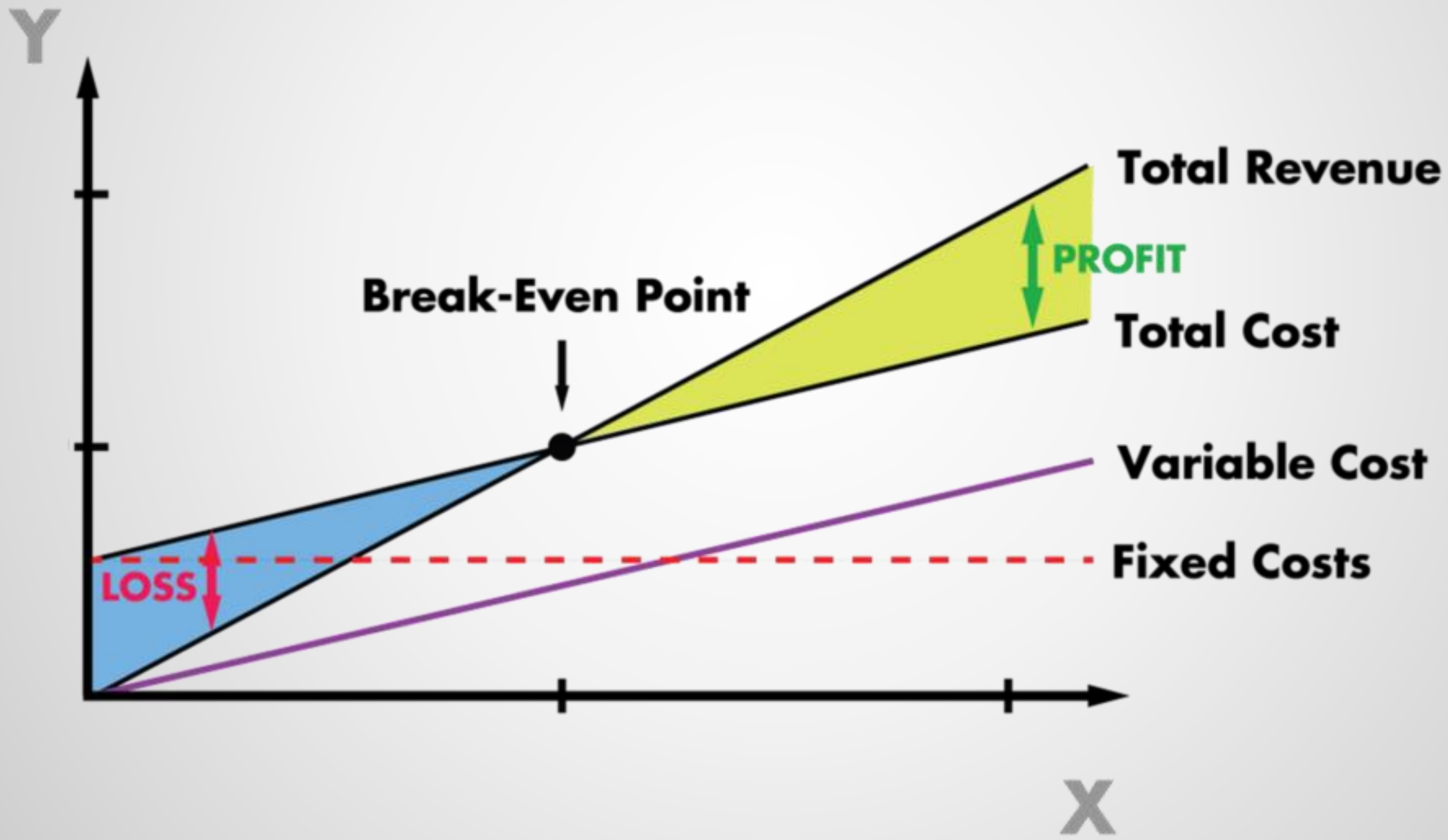
Scales Linear

1D Average

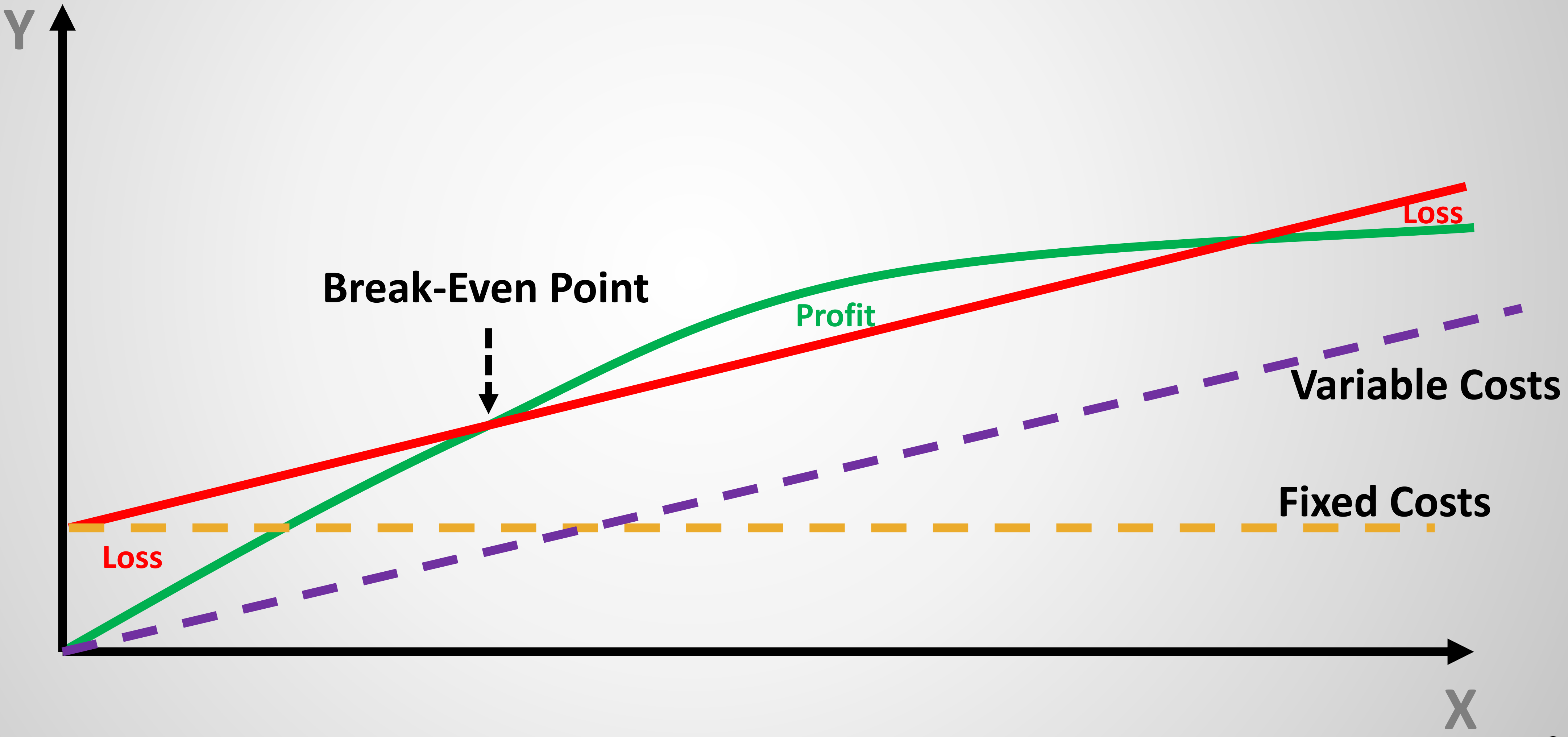
Type Line

Colors

Back to the Profitability Chart



A Little More Realistic Profitability Chart



Still There is a Lot Left to Consider

There are a lot of other economic factors that one should model, some of which are uncertain:

- Selling price of the hardware when the mining project is finished.
- The value/price of the crypto during or at the end of the mining process (remember, you are rewarded in coins, not USD).
- The changes in the price of electricity or other costs (e.g. summer times have more air conditioning expense).
- ….

Mining Hardware

Mining Equipment

So the more computational power you have, the more profit you make by gaining rewards.

Mining Hardware/Equipment:

- Central Processing Unit (CPU)
- Graphical Processing Unit (GPU)
- Field Programmable Gate Arrays (FPGA)
- Application-Specific Integrated Circuits (ASIC)

The Threats of Mining-Dedicated Hardware

Mining-dedicated hardware can significantly shift the computational power towards a specific set of people.

Bitcoin’s SHA256 hash rate:

Core i7 3930k (CPU)	GTX680 (GPU)	Bitmain S9j (ASIC)	Bitmain S19 XP (ASIC)
66 MH/s	120 MH/s	14,5 TH/s	141 TH/s

Puzzle Tweaks to Kick ASICs Out

- Some blockchain designers tried to make ASIC mining hard or costly to keep the network power more distributed.
    - Bitcoin is not among them

- To do so, they had to redesign the puzzle/mathematical problem so that making a hardware for it becomes hard or too costly.
    - RandomX
    - Ethash
    - ProgPoW -> KawPow

    ….

Techniques Adopted for ASIC-resistance

1. **Memory-Hard Functions:** ASICs typically excel at performing repetitive computations, but they often struggle with memory-intensive tasks. By designing mining algorithms that require a significant amount of memory, developers aim to level the playing field for CPUs and GPUs. Memory-hard functions, such as the Ethash algorithm used by Ethereum PoW, forces mining hardware to perform many memory operations, making it more difficult and costly to develop specialized ASICs (but costly Antminer E9 pro was built nevertheless).

2. **Random Accesses:** Similar to memory-hard functions, mining algorithms can be designed to have a high degree of random memory accesses. This approach adds unpredictability to the memory access patterns, which makes it challenging to optimize ASICs for specific computations. Random access patterns can hinder ASICs' ability to achieve the high-speed and efficiency gains they typically offer.

3. **Regular Algorithm Updates:** By regularly updating mining algorithms, developers can introduce changes that disrupt the efficiency of existing ASICs. These updates can involve modifying the underlying computational functions, adjusting parameters, or introducing new elements that require hardware modifications or redesign. Regular algorithm updates make it costly and impractical for ASIC manufacturers to keep up with the changes, providing more opportunities for CPU and GPU miners.

4. **Proof of Stake (PoS):** Moving away from proof-of-work (PoW) consensus mechanisms entirely, as in the case of Ethereum's transition to Ethereum 2.0 with PoS, eliminates the need for mining hardware altogether. PoS relies on participants staking their cryptocurrency holdings as collateral to validate and create new blocks, thereby reducing the reliance on computational power and making ASIC mining irrelevant.

Example of an Exception

Despite using memory-hard functions by Ethash (used by Ethereum before switching to PoS), there came ASIC miners for it.

Core i7-7700HQ	RTX 3080 (GPU)	Bitmain Antminer E9 (ASIC)
1.1 MH/s	95 MH/s	2.4 GH/s

What Comes Next …

- We learned about mining economics and the main factors which must be included in the profitability equation in this industry.

- We also saw the differences in mining hardware and how blockchain developers are shaping this industry by their algorithms.

- Thanks for following us through. The course is concluded here.

Thanks

&

Good Luck