NOKIA Bell Labs

On sustainable economic incentives for Blockchains

1st Blockchain Workshop @ DISC – Vienna, Austria

- Fabio Pianese
- 16-10-2017

Public blockchains as macro-economic systems

Costs vs. revenues, social utility vs. private gains

Blockchain: a distributed system with decentralized trust based on a randomized lottery

Used for cryptocurrencies, self-contained economic systems interacting with the world

Q: How does a blockchain system succeed? What makes it sustainable in the long run?

Observing from a very general (and simplistic) macro perspective, we can define

- Costs (C): the total investment in hardware, energy, networking, etc. to make the system run
- Revenues (R): the total amount of compensation paid to the entities running the system
- Private gains (G=R-C): the revenue-cost position of entities running the system
- Social utility (U): does the system do anything reliable & useful for the world in general?

We expect that a public blockchain can reasonably exist if $G>0$, and is sustainable if also $U>0$

Having a look at Bitcoin’s recent history

A successful, sustainable cryptocurrency?

A blockchain based on Proof-of-Work (PoW) has C and R we can roughly estimate per block:

$$C = \frac{H}{\xi_H} P_W t \qquad\qquad R = (\kappa + \Phi T) P_X$$

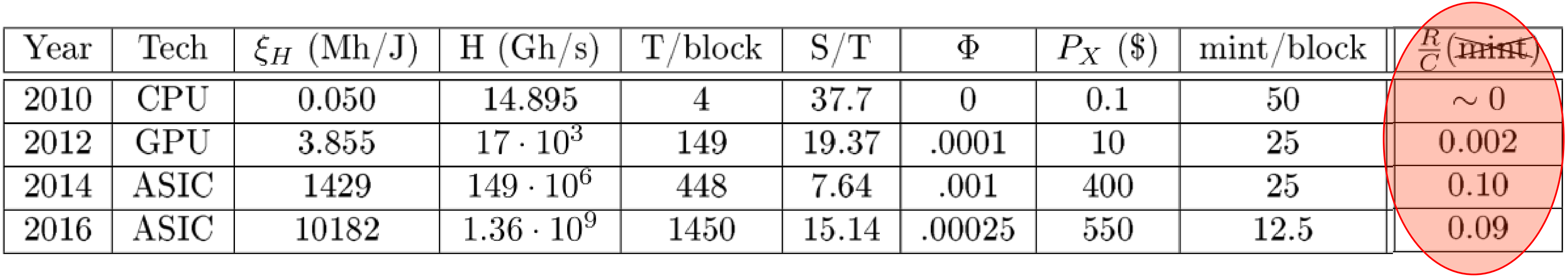
Neglecting the cost of hardware deployment and connectivity, **costs** are driven by energy expenditure (P_W), deployed hash rate (H), HW hash efficiency (ξ_H), & block time (t)

Revenues are determined for each block by minting (k) and collected average fees (Φ) times the number of transactions (T), multiplied by the exchange rate (price) of a Bitcoin (P_X)

Social utility is harder to quantify, and is related to the number (T) and volume (V) of transactions, and if the system provides a reliable service to the world (more on this later)

Bitcoin's economic success

A boon for miners and early adopters!



Year	Tech	ξ_H (Mh/J)	H (Gh/s)	T/block	S/T	Φ	P_X (\$)	mint/block	$\frac{R}{C}$ (~~mint~~)
2010	CPU	0.050	14.895	4	37.7	0	0.1	50	~ 0
2012	GPU	3.855	$17 \cdot 10^3$	149	19.37	.0001	10	25	0.002
2014	ASIC	1429	$149 \cdot 10^6$	448	7.64	.001	400	25	0.10
2016	ASIC	10182	$1.36 \cdot 10^9$	1450	15.14	.00025	550	12.5	0.09

2010: hobbyists were barely breaking even, few transactions were ever made

10x gap in revenue from transactions alone! G<0

...but then the bubble started inflating!

2012-2014: enormous margins of gain, ~500% return on costs, fees are small (\$0.xx)

2016: margins reducing but still high (~200%), fees growing (~\$), T rate starts stagnating

2017: Bitcoin price fluctuating wildly (\$3k-5k), fees >\$, average transactions become bigger

Social utility: why does Bitcoin work in the real world?

Expectations, perceptions, revenue and sustainability - deeply interlocked

Miner participation is rewarded:

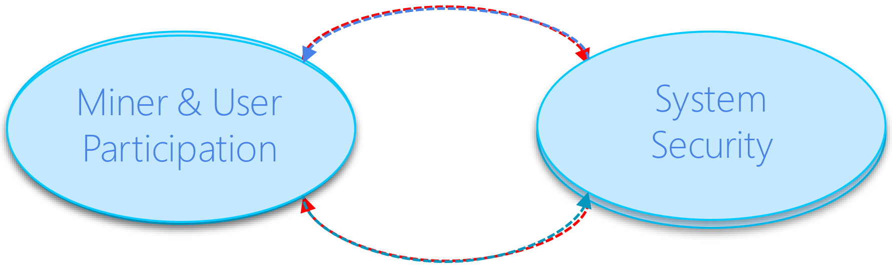
- Contribution to the system entitles miners to receive coins (e.g., for "mining" blocks)
- The security of the blockchain is bolstered by the computational PoW effort from miners

The system is perceived as useful and secure:

- Users have increasing confidence and Bitcoin's adoption and usefulness grow
- Speculative bubbles inflate the value of coins, miners join the system expecting gains

Virtuous cycle

Vicious cycle



Positive feedback

Bitcoin’s incentive design pitfalls

A brief but daunting survey

Transaction fees (as in today’s Bitcoin) thrive on scarcity of “block real estate”

This is bad for several reasons:

- Fee proportionality cannot be enforced if block space abundant (rational miners drive fees down)
- Limits transaction rate by discouraging consensus on the adoption of larger blocks (->BTC forks)
- Fee “by Tx byte” has little relationship to transaction’s value (unfairness on fee/value proportion)
- Also produces unfairness on transaction processing time (more on this in Sara Tucci’s talk)
- Can be exploited to “bribe” nodes into mining on a specific branch (“unstable with no block fee”)

But there are subtler risks with the whole “getting paid for mining” concept:

- Immediate reward is largely independent to social utility U, if block reward prevails over Tx fees
- Hoarding mined currency removes currency from the “useful” economy, reducing Tx rate/volume

Towards new incentive schemes for public blockchains
Ensure long-term sustainability of cryptocurrencies

Carefully pick what behavior to reward and how (as mentioned in talks on earlier session):

- *What to reward*: mining, verification, ownership of coins, overall economic activity?
- *How to reward it*: creating coins, collecting transaction fees, delaying reward?
- *How much to reward it*: coin's monetary value vs. cost of operating the blockchain?

Our proposed solution (work in progress at Bell Labs)

- Enforces proportionality of fees to transactions via demurrage (nominal coin devaluation)
  - Unlike Bitcoin, we do not penalize small payments by fixing a fee: fee % enforces maximum delay
- Introduces conditionality of mining reward on the activity of the system (transactions made)
  - "External incentive" mediated by entity that provides compensation to miners for lending coins
- Blockchain can be purged of older blocks and has bounded maximum size ("sliding window")

"Incentives are the hardest thing to do" -- S. Micali

NOKIA

Copyright and confidentiality