Green Mining: toward a less energetic impact of cryptocurrencies

Philippe Jacquet (Nokia Bell Labs)
Bernard Mans (Macquarie University)
Blockchain workshop 2019
June 12
LINCS, Paris

Energy wasted by Bitcoin

- 40 G kWh/year
- A country like Greece
- 6% France
- 0.25% World

Proof of Work

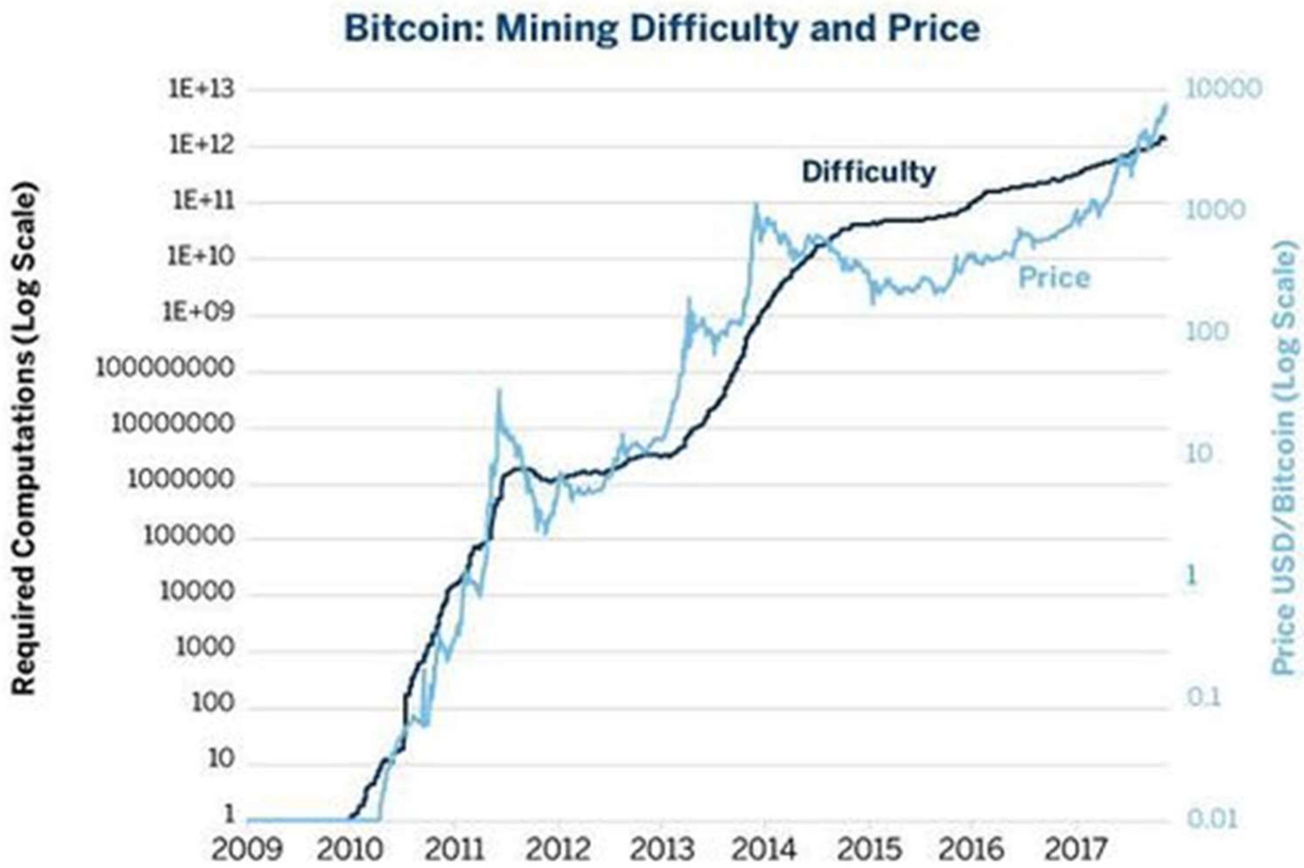
- Each block miner must find a hash value with 74 initial zeroes out of 256 bits.

Field #	**value**
1	Hash of previous block
2	date
3	Transaction refs
4	nonce
5	Hash value

- Difficulty is adjusted in order to have
  - 10 mn inter-block time in average

Evolution of difficulty

- Change every 2016 blocks (approx 2 weeks)

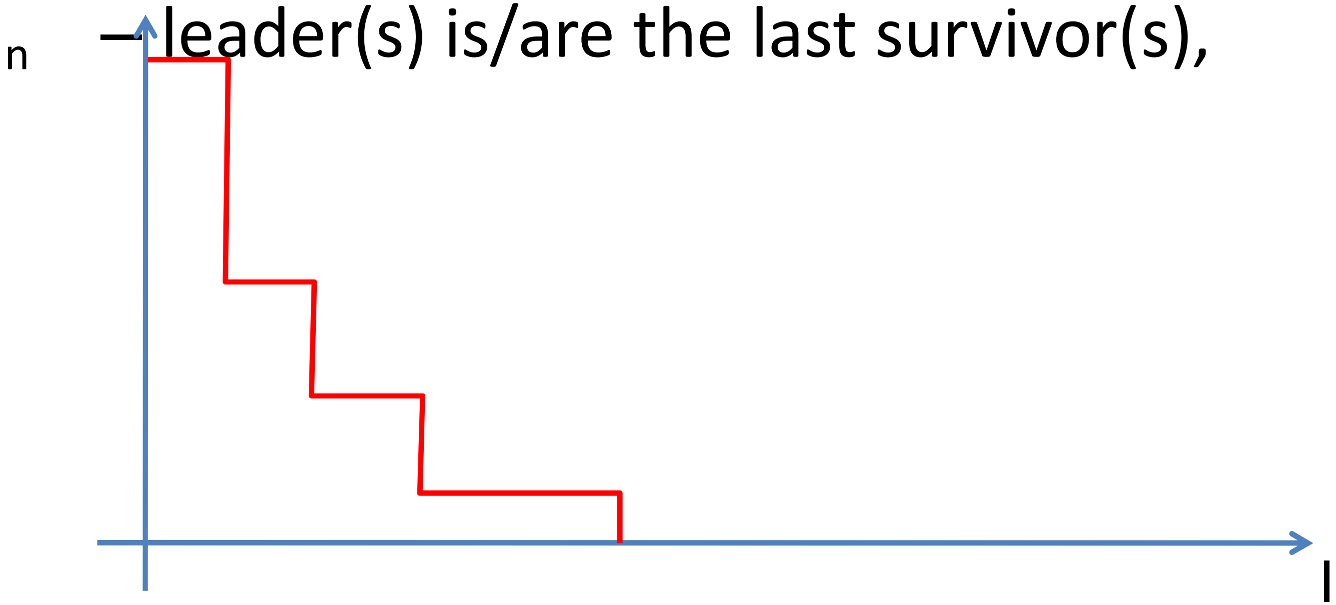


Alternative to PoW

- The block mining via Inversed leader election

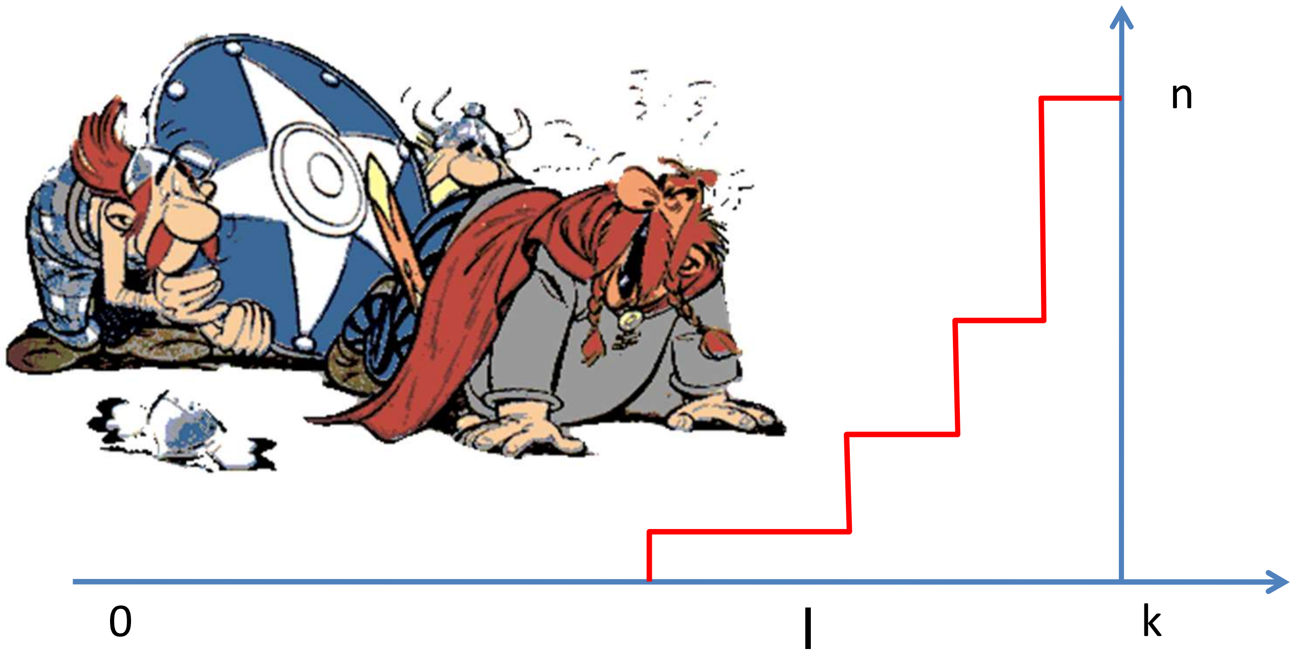
Direct leader election

- n initial competitors a probability p.
  - Eg $n=10^6$, $p=0.5$
  - At each step survivors survive with probability p p^l
  - Process stops when # survivors=0
  - leader(s) is/are the last survivor(s),



Reverse leader election

- Take k such that $p^k n \ll 1$
  - At each step leaders selected with proba p^{k-l}
  - Process stops when # leaders>0



Properties of reverse leader election

- For $n<p^{-k}=N$ the number of leaders (block mined per election) M_n is bounded in distribution
  - $E[M_n] < \min\{n, AN^{1/k}\}, \quad A \approx \frac{1}{\log(1/p)}$
  - For $N=2^{32}$ and k=16: less than 4
  - For n>N $E[M_n] > np$
- N and p fixed as initial parameters,
  - no need to review and update every 2016 blocks

Green mining format

- Regular block

#field	value
1	Previous block hash
2	date
3	Transactions ref
4	Next block call value
5	Block hash

- Next block call value field in regular block
  - It replaces nonce field
  - is fixed by protocol to be $2^{256}/N$
  - Next regular block should have hash value smaller than previous block call value.

Empty blocks

- With $N=2^{32}$ the difficulty is not very big
  - But no nonce to tune
  - The hash value can only be modified by modifying the transaction references. More difficult!
- Virtually impossible to have a hash value smaller $2^{256}/N$. (or take $N=2^{64}$)
  - After one minute an empty block is inserted with a call value higher by a factor $1/p$.

Empty blocks

#field	Field value
1	Hash of previous block
2	date
3	Next block call value
4	Block hash

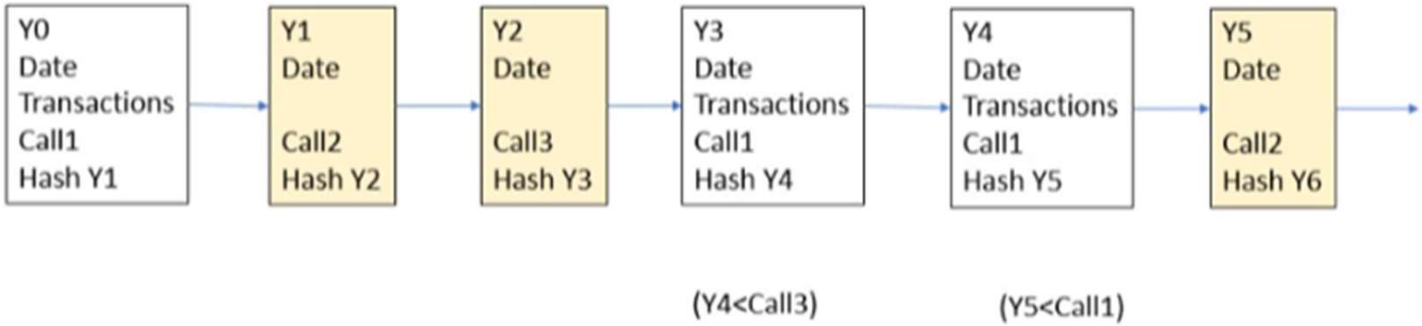
If no regular block is mined after one minute,
    a new empty block is mined
    with call value =previous call value/p
The process restarts after k rounds (call value reaches 2^{256}-1)

Empty blocks

#field	Field value
1	Hash of previous block
2	date
3	$2^{2\text{[illegible]}}-1$
4	Block hash

Last call value releases all blocks

Empty blocks mining



- Empty block mining options
  - Can be mined by a central entity
  - Can be mined in a decentralized mode
    - Filtered by the block dates
  - Implicit empty block mining
    - Regular blocks filtered by hash values and dates

Performance analysis

- Explicit empty block mining
- Theorem [explicit empty blocks]:

$$E[M_n] = np^k + \sum_{\ell=1}^{k} np^{k-\ell} \prod_{i<\ell} (1 - p^{k-i})^n$$

  – Proof: the probability to reach round ℓ is $\prod_{i<\ell} (1 - p^{k-i})^n$

- Lemma

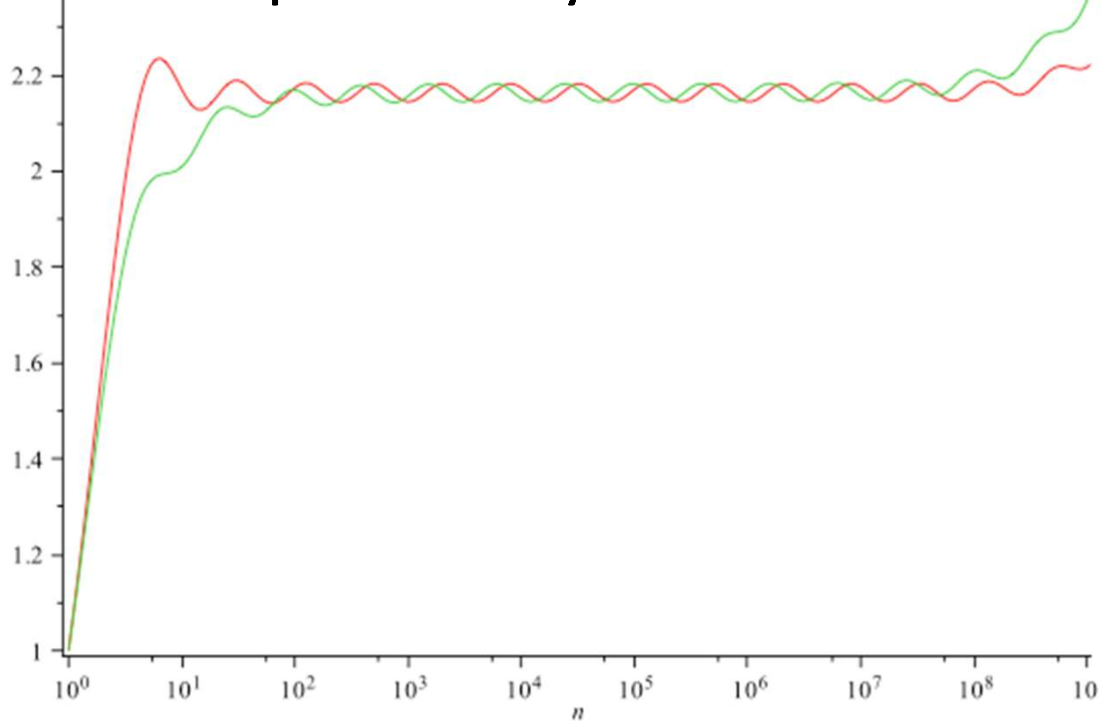
$$\sum_{\ell=1}^{k} np^{k-\ell} \prod_{i<\ell} (1 - p^{k-i})^n \leq \frac{1}{p} \sum_{\ell \in Z} np^{\ell} \exp\left(-np^{\ell}\right) = O\left(\frac{1}{p}\right) = O(N^{1/k})$$

Performance analysis (continued)

- Theorem [implicit empty blocks]:

$$E[M_n] = np^k + \sum_{l=1}^{k} n(p^{k-l} - p^{k-l+1})\left(1 - p^{k-l+1}\right)^{n-1}$$

  – Proof the probability to reach round l is $\left(1 - p^{k-l+1}\right)^n$



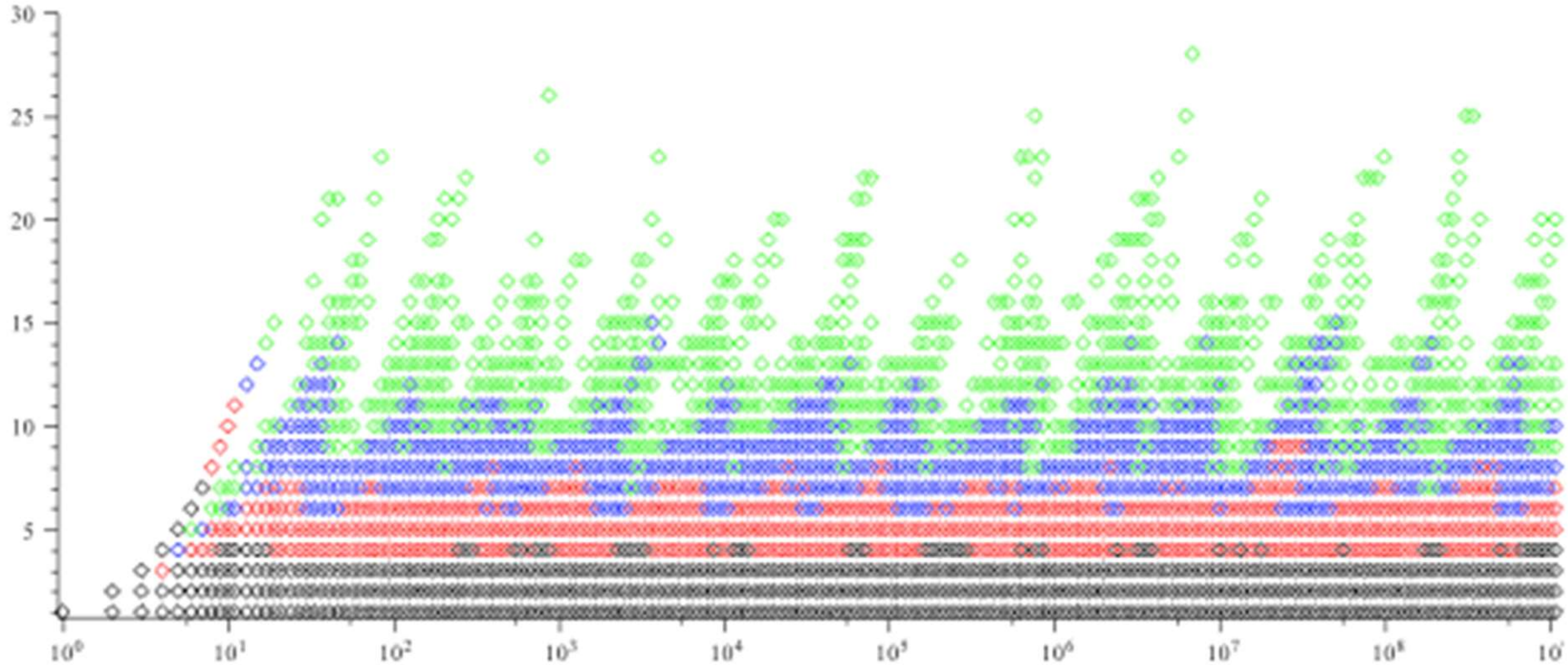
Performance analysis (continued)

- Theorem distribution of number of mined blocks [explicit empty blocks]:

$$
\begin{aligned}
E\left[u^{M_n}\right] = {} & (1+p^k(u-1))^n - (1-p^k)^n \\
& + \sum_{l<k} \left((1+p^{k-l}(u-1))^n - (1-p^{k-l})^n \right) \prod_{j<l} (1-p^{k-j})^n \\
& + u^n \prod_{j<k} (1-p^{k-j})^n
\end{aligned}
$$

Performance analysis (end)

- Simulation of green mining



Conclusion

- The Energy waste due to proof of work is not sustainable in cryptocurrencies in the near future.
- A reversed leader election can replace the burden of the PoW for mining difficulty
- Highly dynamic, work for any mining population up to N (arbitrary large)
- No need of parameter update

Perspective

- How resilient is the scheme against attack
- Eg 51% attack.
  - block nursing vs PoW farming
  - Preliminary analysis indicates
    - to get ε advantage one should need $2\varepsilon\log(1/p)$ more resources than the adversary