Bitcoin – The Actual Cost (energy)

Jay Babin

E-Flow (Thailand) Co. Ltd.

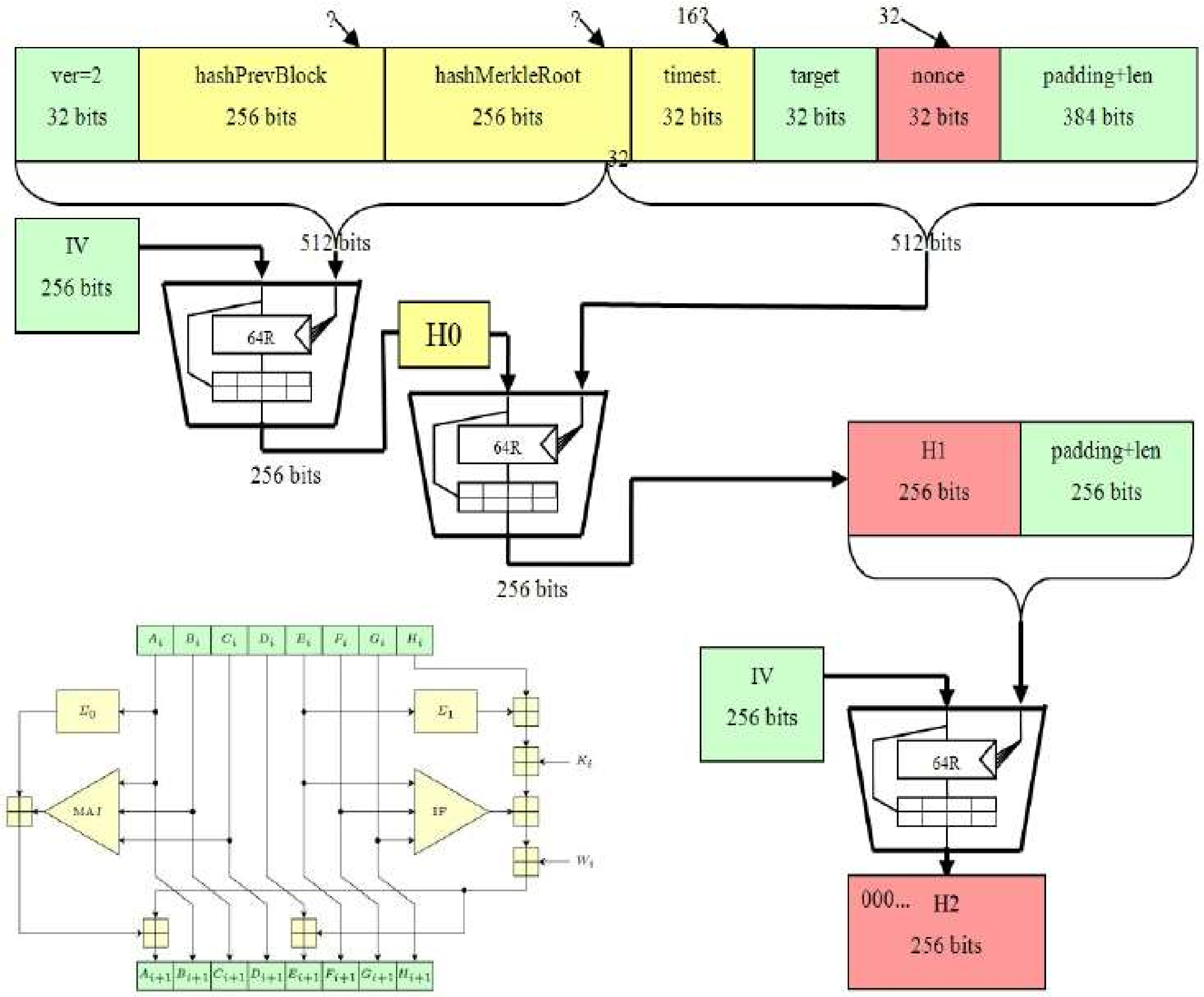
E-Flow (Thailand) Co. Ltd.

Bitcoin History/Facts

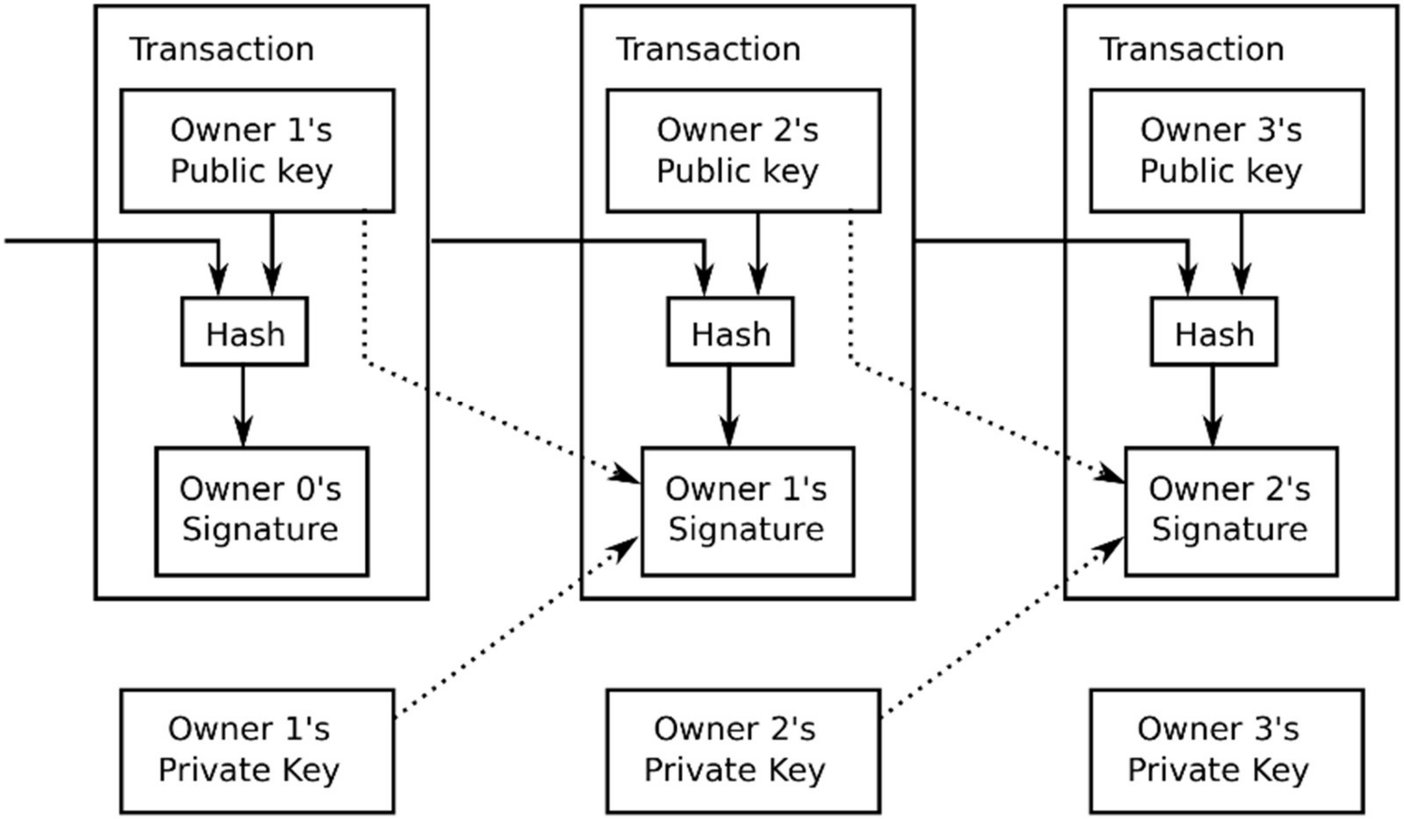
- Created in in 2008 by Satoshi Nakamoto (unknown person/group)
- Began use in 2009
- In 2010, the first known commercial transaction using bitcoin occurred when programmer Laszlo Hanyecz bought two Papa John's pizzas for ฿10,000 from Jeremy Sturdivant
  - Current vale @ $21,500 each = $215,000,000
- in 2013 one user claimed to have lost ฿7,500, worth $7.5 million at the time, when he accidentally discarded a hard drive containing his private key. About 20% of all bitcoins are believed to be lost -they would have had a market value of about $20 billion at July 2018 prices

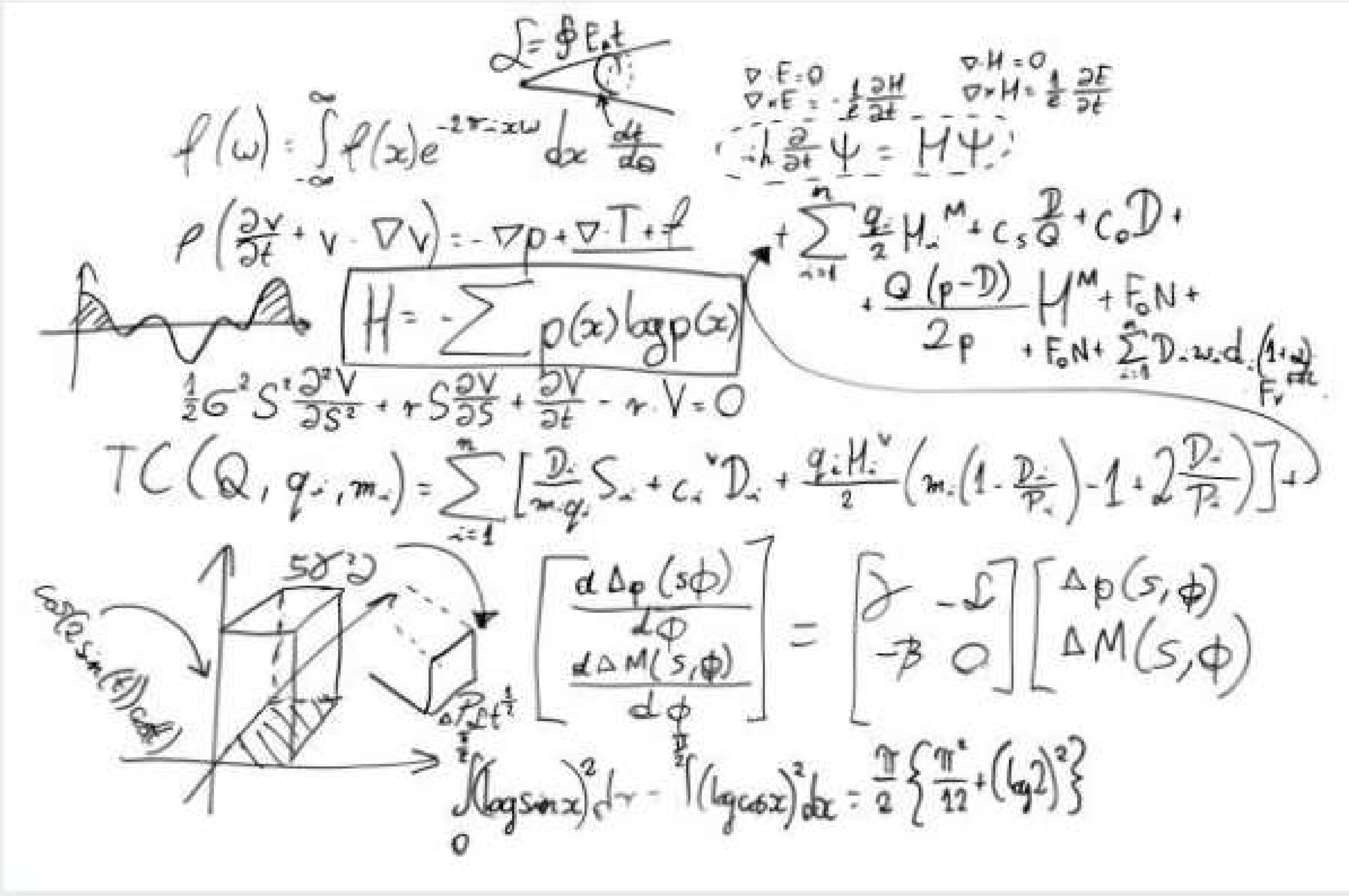
Bitcoin History/Facts

- Uses “Proof of work” blockchain technology
- The bitcoin blockchain is a public ledger that records bitcoin transactions. It is implemented as a chain of *blocks*, each block containing a cryptographic hash of the previous block up to the genesis block in the chain. A network of communicating nodes running bitcoin software maintains the blockchain. Transactions of the form *payer X sends Y bitcoins to payee Z* are broadcast to this network using readily available software applications.

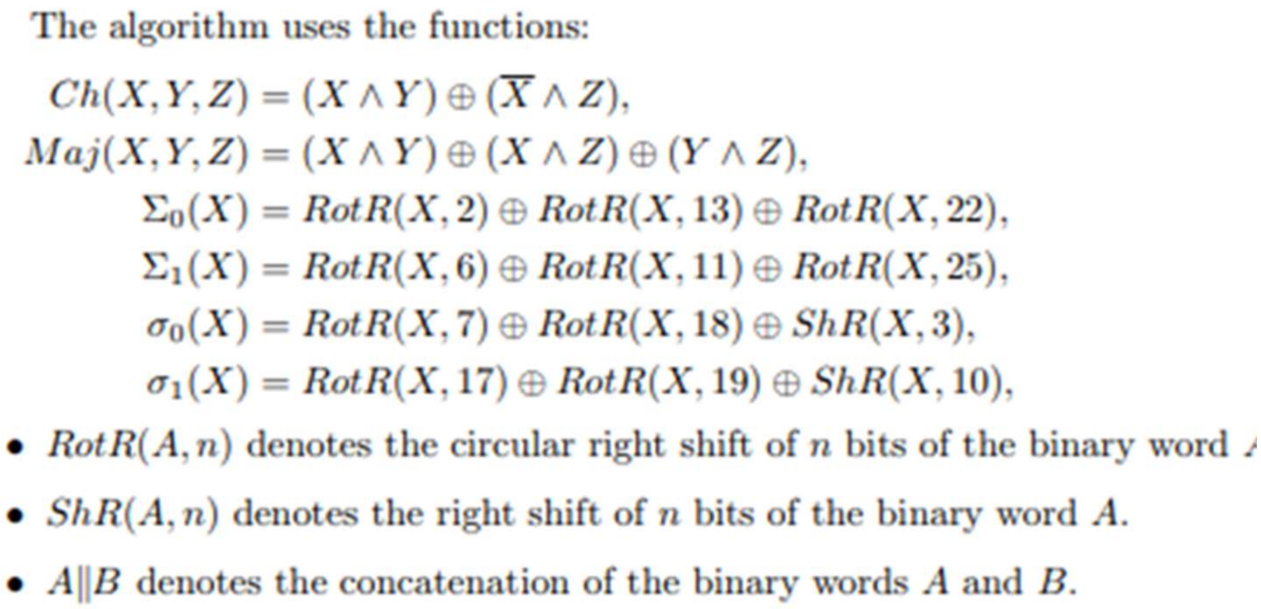


?
?
16?
32
ver=2
32 bits
hashPrevBlock
256 bits
hashMerkleRoot
256 bits
timest.
32 bits
target
32 bits
nonce
32 bits
padding+len
384 bits
32
512 bits
512 bits
IV
256 bits
64R
H0
256 bits
64R
H1
256 bits
padding+len
256 bits
256 bits
IV
256 bits
64R
000...
H2
256 bits
A_i B_i C_i D_i E_i F_i G_i H_i
Σ_0
Σ_1
MAJ
IF
K_i
W_i
A_{i+1} B_{i+1} C_{i+1} D_{i+1} E_{i+1} F_{i+1} G_{i+1} H_{i+1}


Transaction
Owner 1's Public key
Hash
Owner 0's Signature
Transaction
Owner 2's Public key
Hash
Owner 1's Signature
Transaction
Owner 3's Public key
Hash
Owner 2's Signature
Owner 1's Private Key
Owner 2's Private Key
Owner 3's Private Key



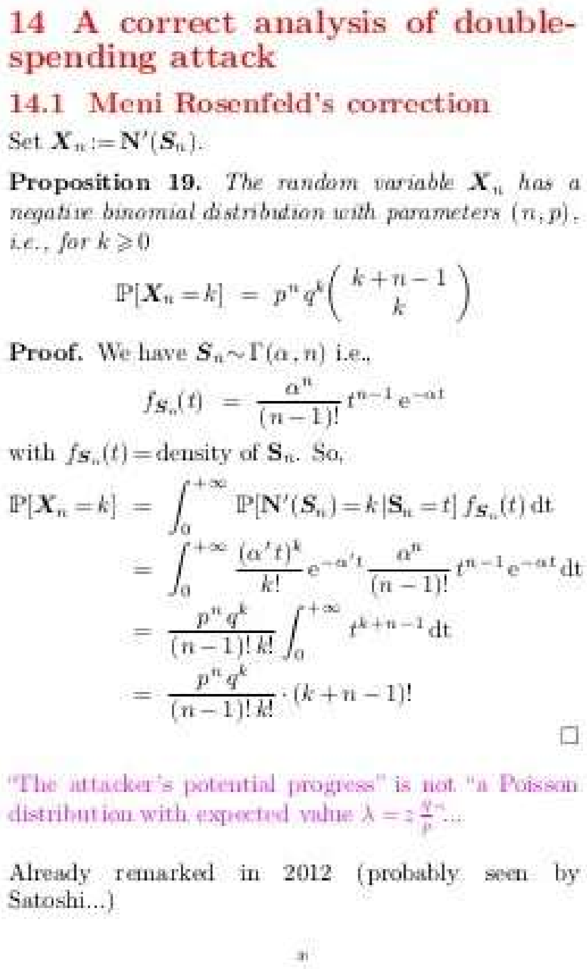
$\mathcal{E} = \oint E\,dt$
$\nabla \cdot E = 0$
$\nabla \times E = -\frac{1}{c}\frac{\partial H}{\partial t}$
$\nabla \cdot H = 0$
$\nabla \times H = \frac{1}{c}\frac{\partial E}{\partial t}$
$f(\omega) = \int_{-\infty}^{\infty} f(x) e^{-2\pi i x \omega} dx \; \frac{dt}{d\theta}$
$i\hbar \frac{\partial}{\partial t}\Psi = H\Psi$
$\rho\left(\frac{\partial v}{\partial t} + v \cdot \nabla v\right) = -\nabla p + \nabla \cdot T + f$
$H = -\sum p(x) \log p(x)$
$+\sum_{i=1}^{n} \frac{q_i}{2} H_i^M + c_s \frac{D}{Q} + c_0 D +$
$+\frac{Q(p-D)}{2p} H^M + F_0 N +$
$+ F_0 N + \sum_{i=1}^{n} D_i w_i d_i \left(1 + \frac{\alpha}{F_r}\right)$
$\frac{1}{2}\sigma^2 S^2 \frac{\partial^2 V}{\partial S^2} + rS\frac{\partial V}{\partial S} + \frac{\partial V}{\partial t} - rV = 0$
$TC(Q, q_i, m_i) = \sum_{i=1}^{n}\left[\frac{D_i}{m_i q_i} S_i + c_i^v D_i + \frac{q_i H_i^v}{2}\left(m_i\left(1 - \frac{D_i}{P_i}\right) - 1 + 2\frac{D_i}{P_i}\right)\right] +$
$5\gamma^2$
$\cos(e\sin(\theta))\cos(\theta)$
$\sigma P_2 t^{\frac{1}{2}}$
$\begin{bmatrix} \frac{d\Delta p(s,\phi)}{d\phi} \\ \frac{d\Delta M(s,\phi)}{d\phi} \end{bmatrix} = \begin{bmatrix} \gamma & -\delta \\ -\beta & 0 \end{bmatrix} \begin{bmatrix} \Delta p(s,\phi) \\ \Delta M(s,\phi) \end{bmatrix}$
$\int_0^{\frac{\pi}{2}} (\log \sin x)^2 dx = \int_0^{\frac{\pi}{2}} (\log \cos x)^2 dx = \frac{\pi}{2}\left\{\frac{\pi^2}{12} + (\log 2)^2\right\}$



The algorithm uses the functions:

$$
\begin{aligned}
Ch(X,Y,Z) &= (X \wedge Y) \oplus (\overline{X} \wedge Z),\\
Maj(X,Y,Z) &= (X \wedge Y) \oplus (X \wedge Z) \oplus (Y \wedge Z),\\
\Sigma_0(X) &= RotR(X,2) \oplus RotR(X,13) \oplus RotR(X,22),\\
\Sigma_1(X) &= RotR(X,6) \oplus RotR(X,11) \oplus RotR(X,25),\\
\sigma_0(X) &= RotR(X,7) \oplus RotR(X,18) \oplus ShR(X,3),\\
\sigma_1(X) &= RotR(X,17) \oplus RotR(X,19) \oplus ShR(X,10),
\end{aligned}
$$

- $RotR(A,n)$ denotes the circular right shift of n bits of the binary word
- $ShR(A,n)$ denotes the right shift of n bits of the binary word A.
- $A \| B$ denotes the concatenation of the binary words A and B.



14 A correct analysis of double-spending attack

14.1 Meni Rosenfeld's correction

Set $\boldsymbol{X}_n := \mathbf{N}'(\boldsymbol{S}_n)$.

Proposition 19. *The random variable $\boldsymbol{X}_n$ has a negative binomial distribution with parameters (n,p), i.e., for $k \geqslant 0$*

$$\mathbb{P}[\boldsymbol{X}_n = k] \;=\; p^n q^k \binom{k+n-1}{k}$$

Proof. We have $\boldsymbol{S}_n \sim \Gamma(\alpha, n)$ i.e.,

$$f_{\boldsymbol{S}_n}(t) \;=\; \frac{\alpha^n}{(n-1)!} t^{n-1} \mathrm{e}^{-\alpha t}$$

with $f_{\boldsymbol{S}_n}(t) =$ density of $\mathbf{S}_n$. So,

$$
\begin{aligned}
\mathbb{P}[\boldsymbol{X}_n = k] &= \int_0^{+\infty} \mathbb{P}[\mathbf{N}'(\boldsymbol{S}_n) = k \,|\, \mathbf{S}_n = t]\, f_{\boldsymbol{S}_n}(t)\,\mathrm{dt}\\
&= \int_0^{+\infty} \frac{(\alpha' t)^k}{k!} \mathrm{e}^{-\alpha' t} \frac{\alpha^n}{(n-1)!} t^{n-1} \mathrm{e}^{-\alpha t}\,\mathrm{dt}\\
&= \frac{p^n q^k}{(n-1)!\,k!} \int_0^{+\infty} t^{k+n-1}\,\mathrm{dt}\\
&= \frac{p^n q^k}{(n-1)!\,k!} \cdot (k+n-1)!
\end{aligned}
$$

□

"The attacker's potential progress" is not "a Poisson distribution with expected value $\lambda = z\frac{q}{p}$...

Already remarked in 2012 (probably seen by Satoshi...)

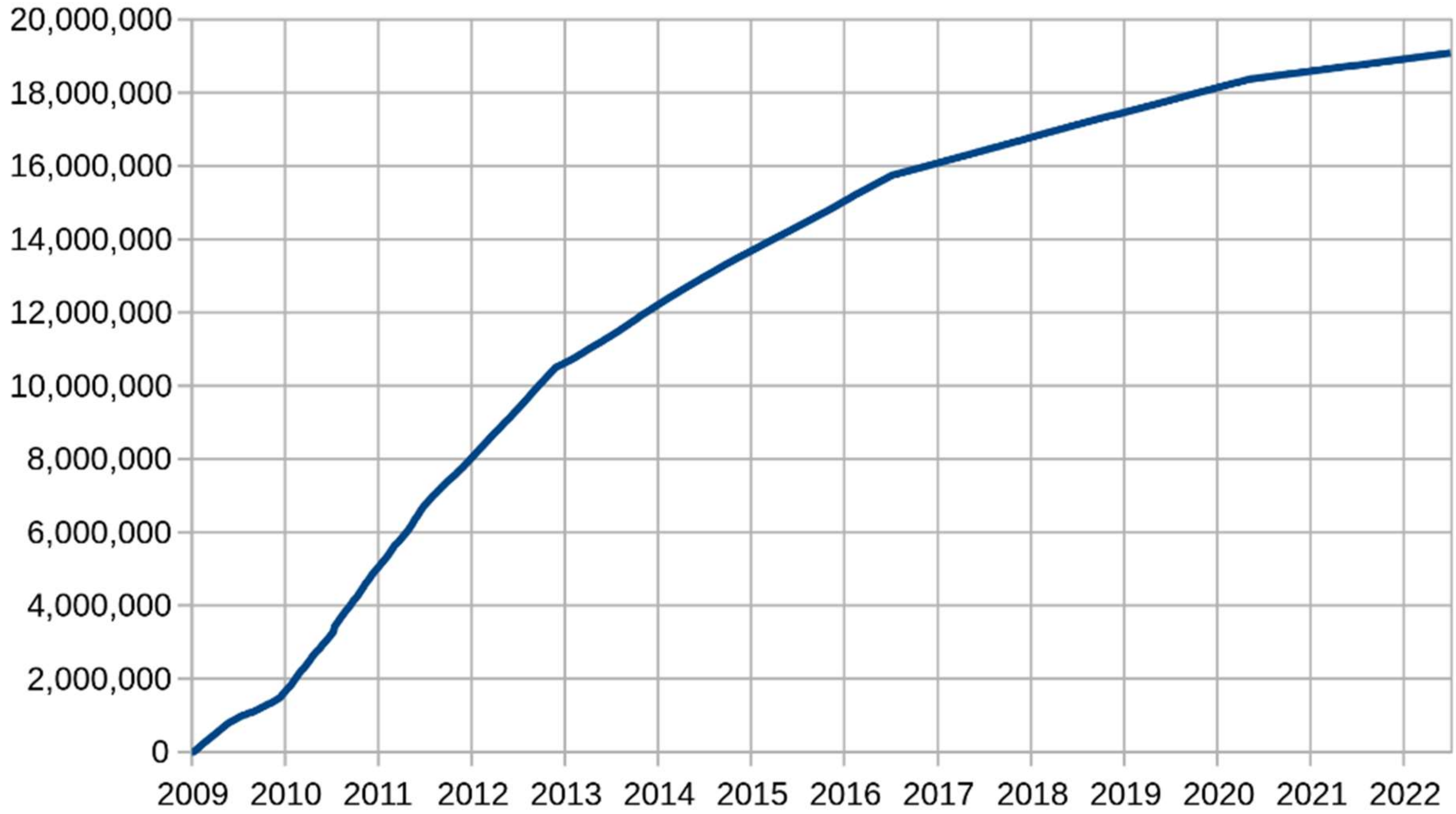
bitcoin is "backed by math"

Bitcoin Mining

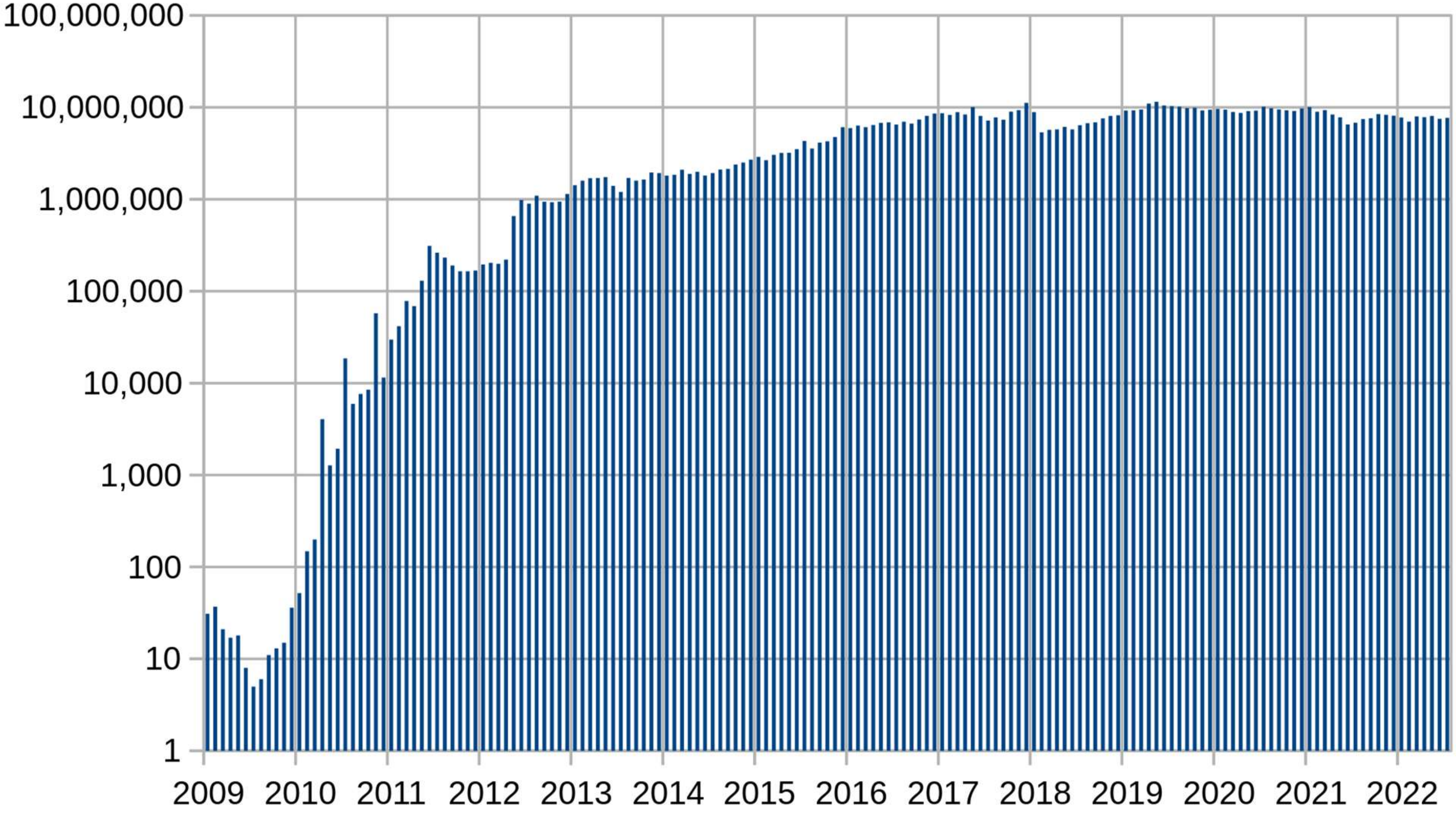
- Solving the block hash currently gets you 6.25 bitcoins
- First to solve it wins

- As of April 2022, it takes on average 122 sextillion (122 thousand billion billion) attempts to generate a block hash smaller than the difficulty target.

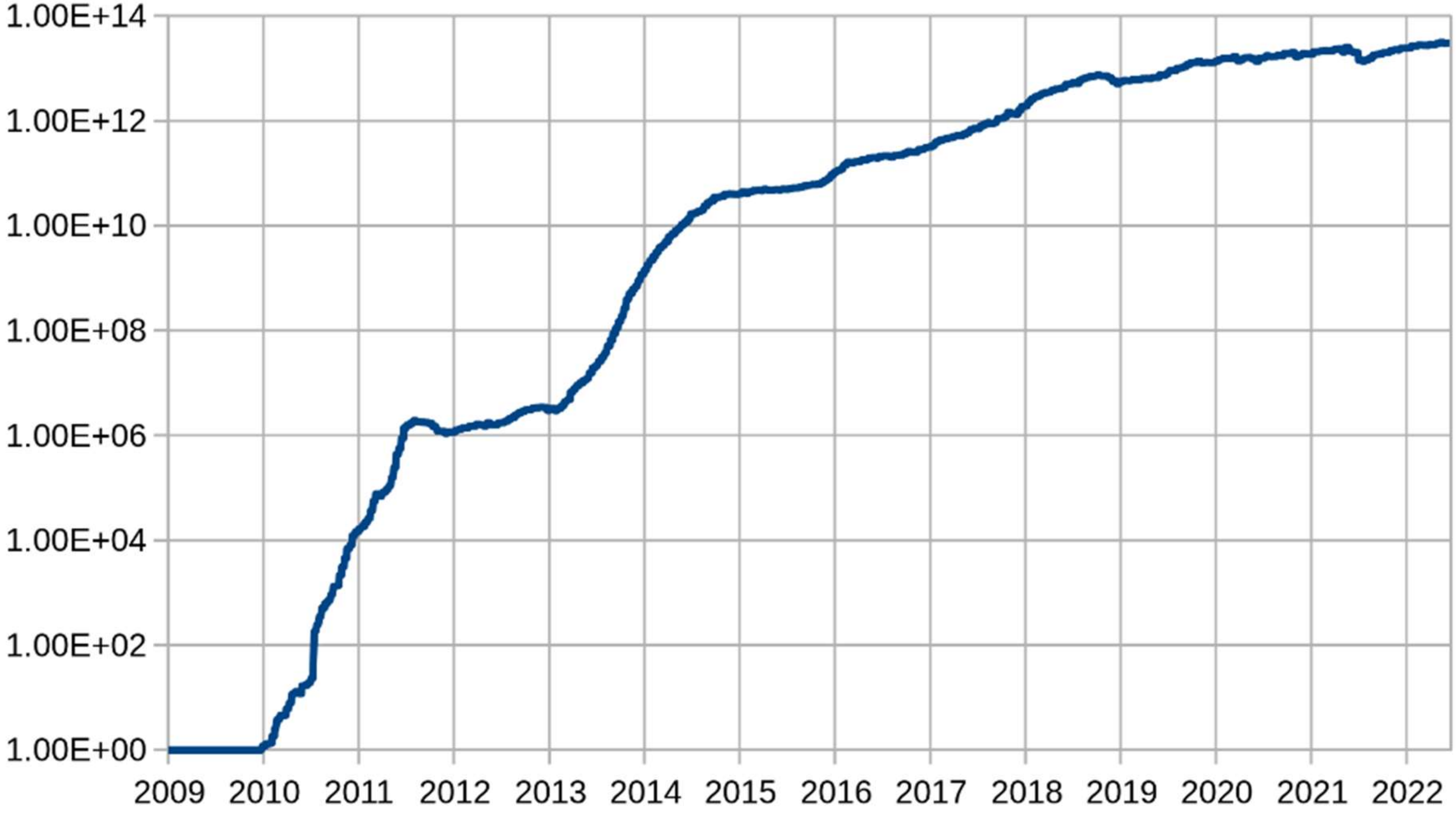
Total Bitcoins in Circulation *ref: Ladislav Mecir*



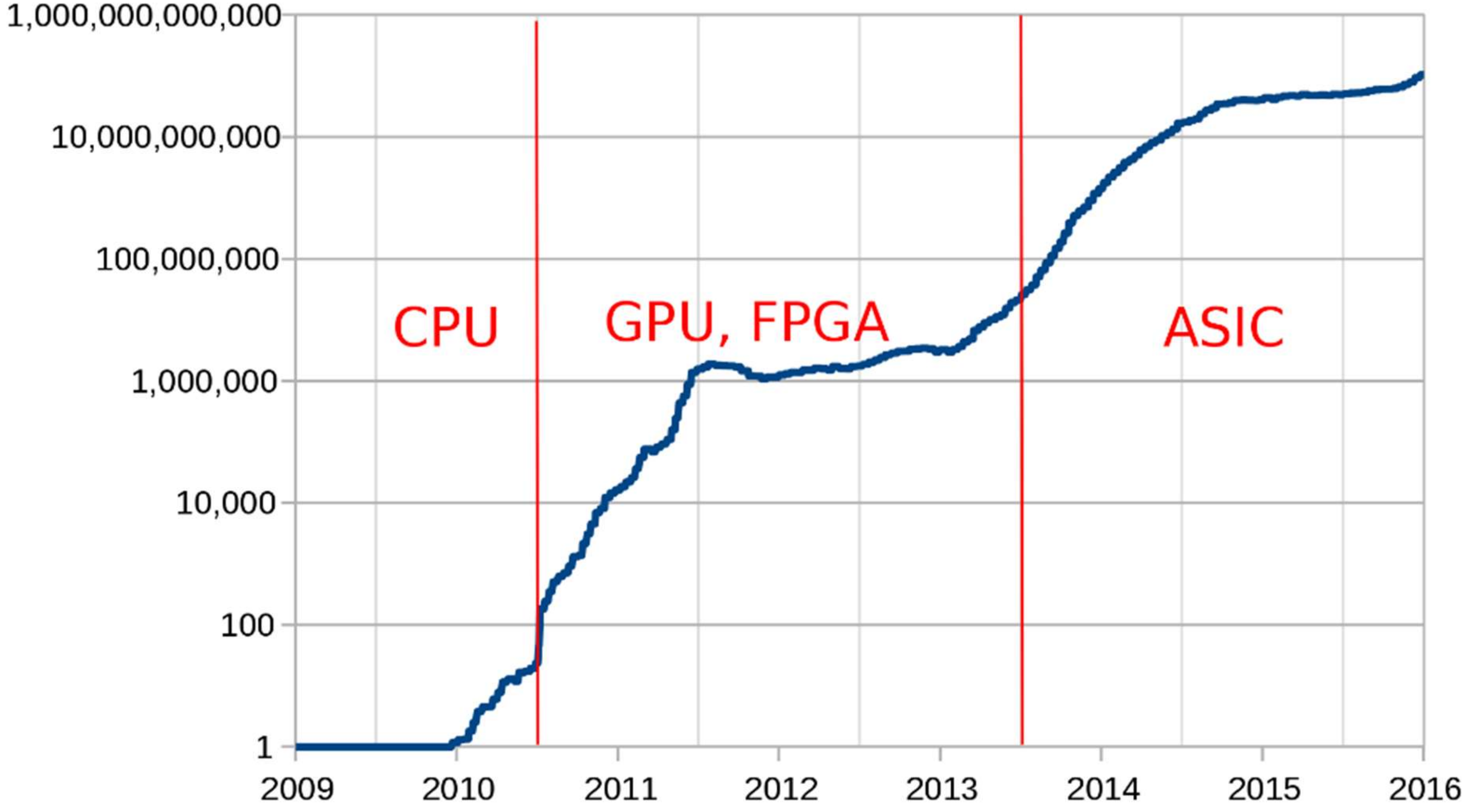
Bitcoin Transactions/month *ref Ladislav Mecir*



Bitcoin mining difficulty *ref Ladislav Mecir*



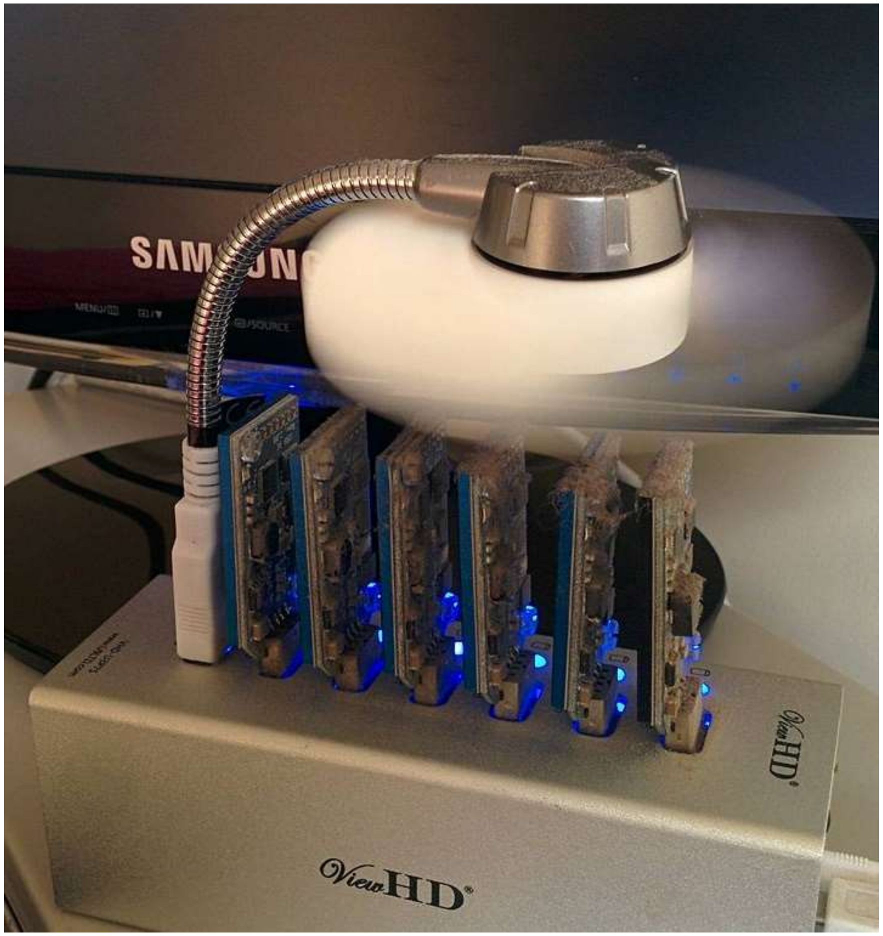
Bitcoin mining difficulty *ref Ladislav Mecir*



1st generation mining used CPUs

2nd generation mining equipment used GPUs

3rd generation mining using FPGA and ASIC chips



Ant Miner S9. 1,323 W. Amazon. $799 ea

Russia

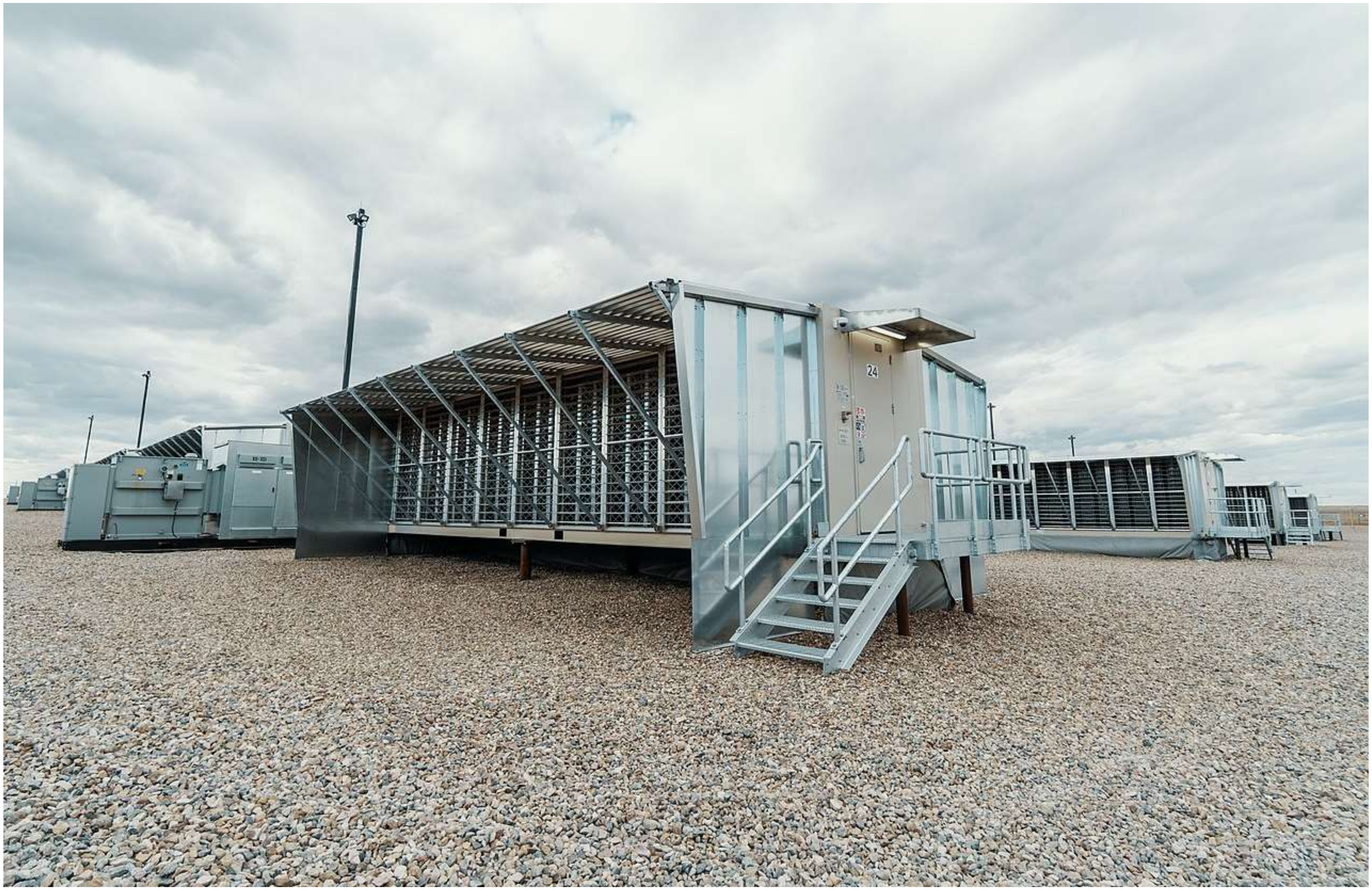
Russia

A crypto mining farm in Nadvoitsy, Russia.

Getty Images

Argentina

Medicine Hat, Alberta



TECHNOLOGY

The Cost of Mining Bitcoin in 198 Different Countries

Published 1 month ago on August 5, 2022

By NeoMam Studios ✓ Featured Creator Article/Editing: Carmen Ang

- It takes an estimated 1,449 kilowatt hours (kWh) of energy to mine a single bitcoin. That’s the same amount of energy an average U.S. household consumes in approximately 13 years.
  - 9.3 kWh/month

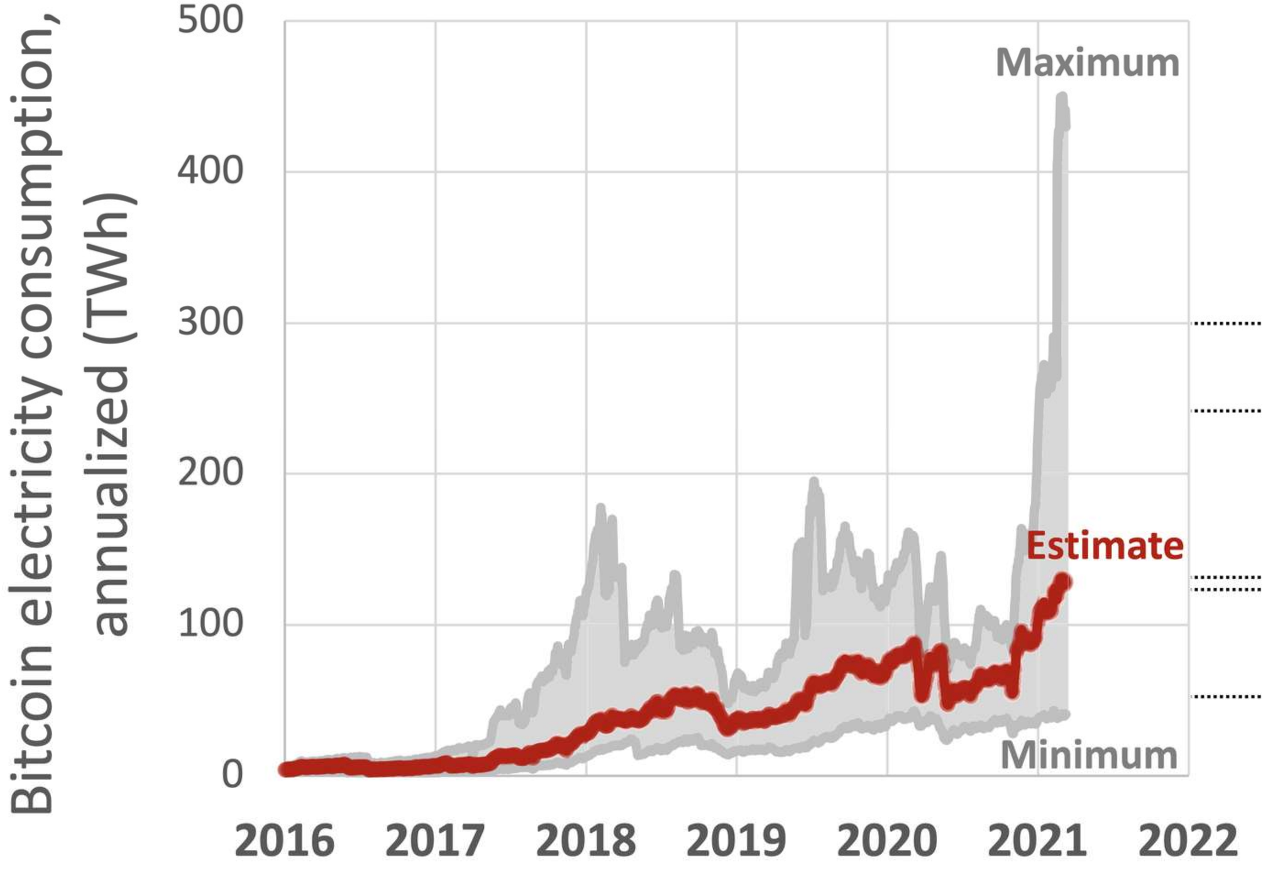
- My house uses approx. 500 kWh/month
- Thai houses aren’t the same as US houses!!!!!

Bitcoin energy consumption

- The Digiconomist's Bitcoin Energy Consumption Index estimated that one bitcoin transaction takes 1,449 kWh to complete, or the equivalent of approximately 50 days of power for the average US household
  - *Ref* CNET, Oscar Gonzalez July 18, 2022

- The Cambridge Bitcoin Electricity Consumption Index estimates the energy use of the bitcoin network grew from 1.95 terawatt-hours per year at the end of 2014, to 77.1 terawatt-hours per year by the end of 2019.

- As of 2022, the Cambridge Centre for Alternative Finance (CCAF) estimates that Bitcoin consumes 131 TWh annually, representing 0.29% of the world's energy production and 0.59% of the world's electricity production, ranking Bitcoin mining between Ukraine and Egypt in terms of electricity consumption.



Country equivalent:

UK: 300 TWh

Spain: 242 TWh

Thailand 191 TWh (2019)

Sweden: 131 TWh

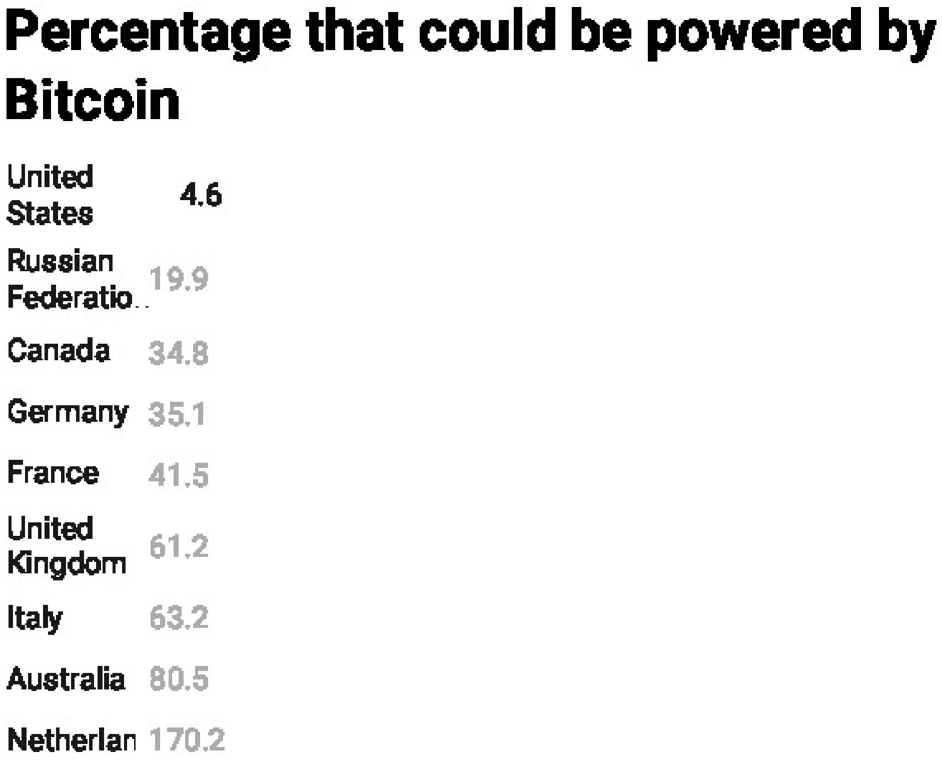
Argentina: 125 TWh

Israel: 56 TWh

Bitcoin electricity consumption based on data from the University of Cambridge (last updated: 11.03.2021. Source: Cambridge Bitcoin Electricity Consumption Index. https://cbeci.org/). Maximum, minimum, and an (estimated) best-guess value are plotted over time and compared to the electricity consumption of various countries.

Energy Consumption Comparison

DIGICONOMIST



Percentage that could be powered by Bitcoin

United States	4.6
Russian Federatio...	19.9
Canada	34.8
Germany	35.1
France	41.5
United Kingdom	61.2
Italy	63.2
Australia	80.5
Netherlan	170.2

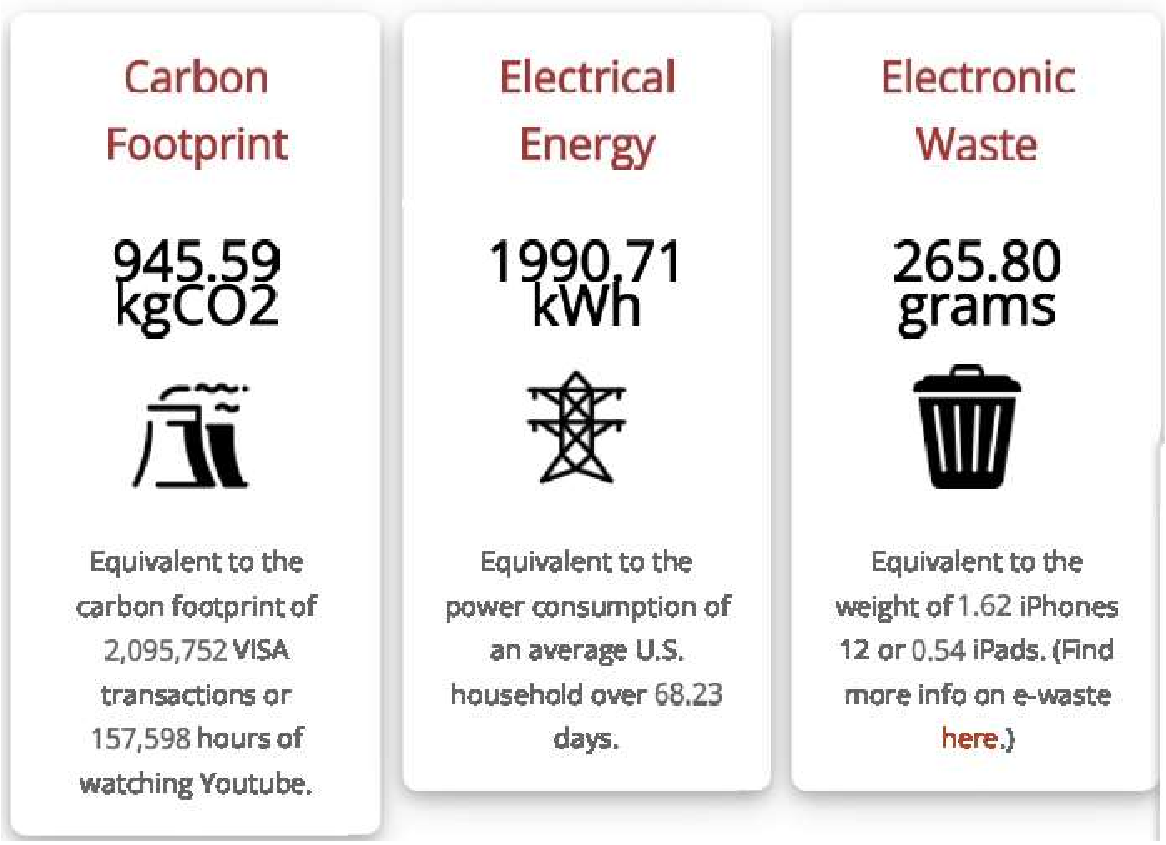
Bitcoin Energy Consumption

- In June 2021 China banned Bitcoin mining
- By December 2021, most mining was done in the U.S. (35.4%), Kazakhstan (18.1%), and Russia (11%)

- According to studies published in 2019 , Bitcoin's annual energy consumption results in annual carbon emission ranging from 17 to 22.9 $MtCO_2$ which is comparable to the level of emissions of countries as Jordan and Sri Lanka or Kansas City
  - *Köhler, Susanne; Pizzol, Massimo (20 November 2019). "Life Cycle Assessment of Bitcoin Mining". Environmental Science & Technology. **53** (23): 13598–13606.*

Single Bitcoin Transaction

DIGICONOMIST



Carbon Footprint

945.59 kgCO2

Equivalent to the carbon footprint of 2,095,752 VISA transactions or 157,598 hours of watching Youtube.

Electrical Energy

1990.71 kWh

Equivalent to the power consumption of an average U.S. household over 68.23 days.

Electronic Waste

265.80 grams

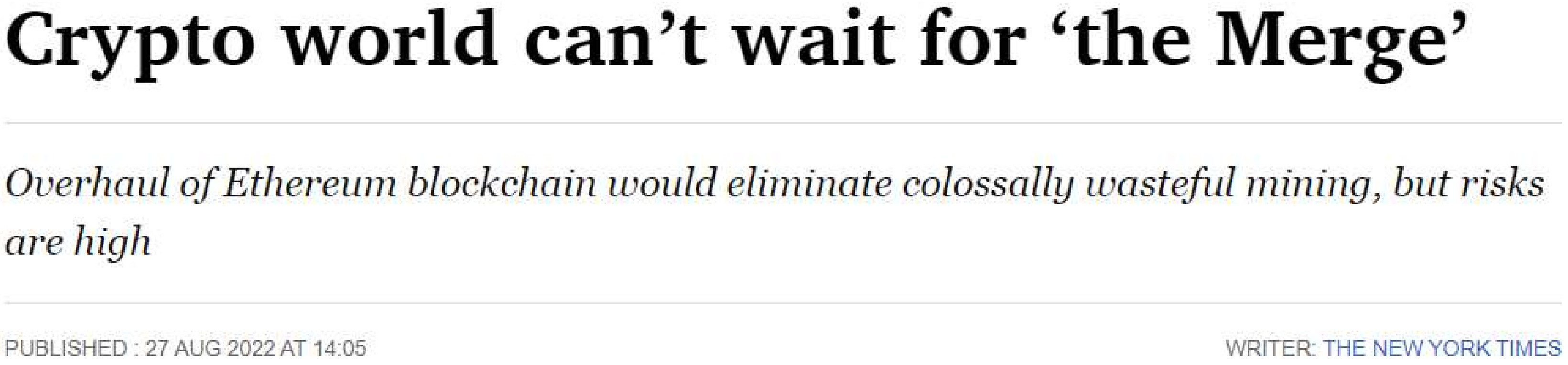
Equivalent to the weight of 1.62 iPhones 12 or 0.54 iPads. (Find more info on e-waste here.)

Bitcoin and e-waste

- electronic waste generated by Bitcoin mining devices amounts to 30.7 metric kilotonnes annually.
- the consistent increase of the Bitcoin network's hashrate, mining devices are estimated to have an average lifespan of 1.29 years until they become unprofitable and need to be replaced. Mining devices based on ASIC technology are specialized and cannot be repurposed for another use, and hence become electronic waste once they become unprofitable.

  - *Ref* de Vries, Alex; Stoll, Christian (December 2021). "Bitcoin's growing e-waste problem". *Resources, Conservation and Recycling*. **175**: 105901

Future of Blockchain
Proof of Work vs. Proof of Stake



Crypto world can’t wait for ‘the Merge’

Overhaul of Ethereum blockchain would eliminate colossally wasteful mining, but risks are high

PUBLISHED : 27 AUG 2022 AT 14:05 WRITER: THE NEW YORK TIMES

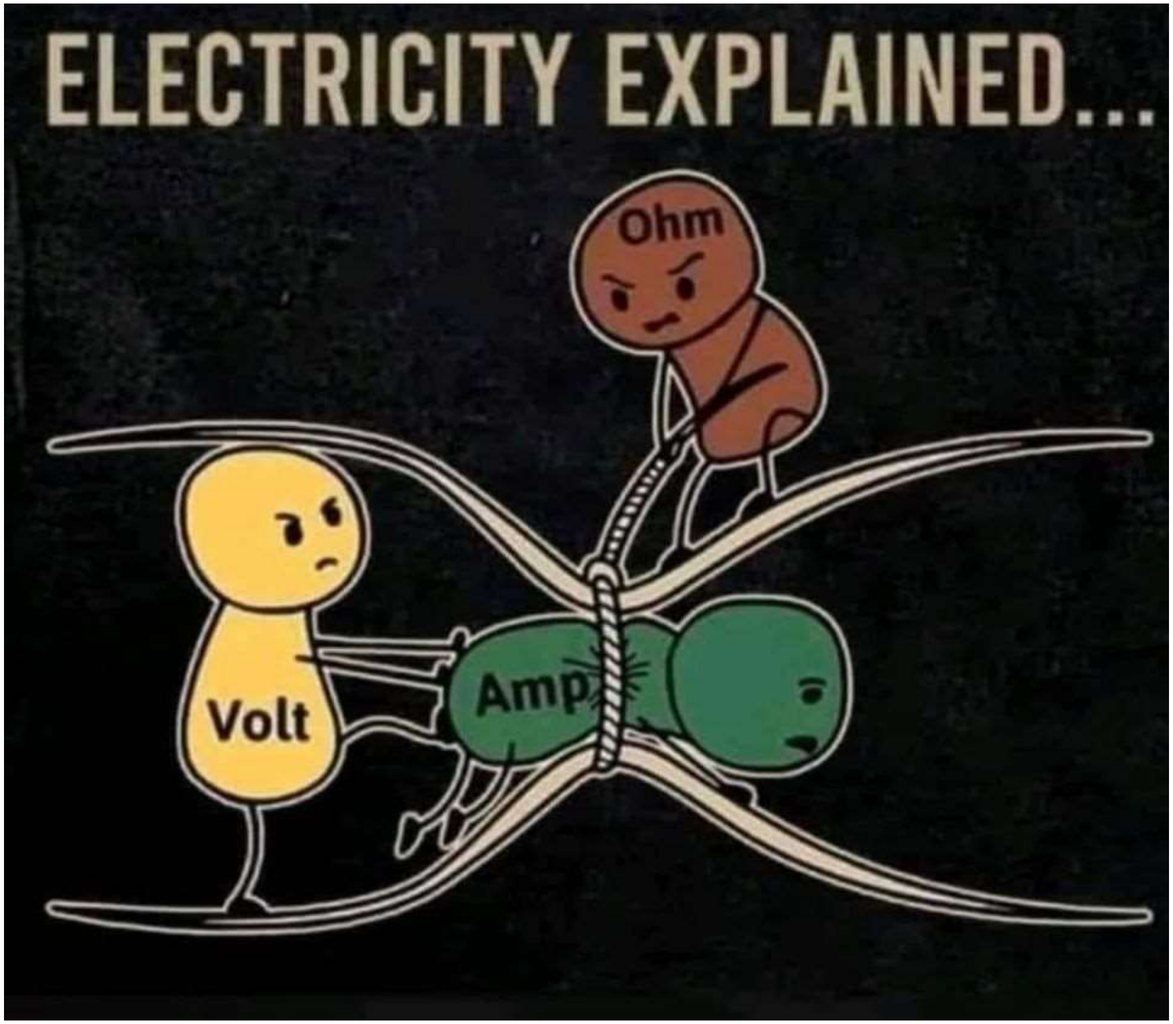
- One computer is selected to do the work, the rest validate it

- Ethereum is set to transition to the new protocol on Sept. 19 (some say Sept. 15), but that date is not final.
- This change should reduce the amount of energy needed for ethereum mining by 99.95%

Summary

- Bitcoin transactions use a lot of energy (~1,500 kWh ea.)
- Total power consumption is a lot 131 TWh/yr
  - Ranked 30th country in the world between Ukraine (133 TWh) and Norway (122 TWh)
- Bitcoin creates a lot of e-waste (265 g (1.2 iPhones))

Electricity Fundamentals



Time Lapse from Kuala Lumpur