

Blockchain applications: an energy perspective

12 April 2022

International Energy Agency

Agenda

14h00	 Welcome and opening remarks Pauline Henriot, 3DEN Lead Analyst, Energy Efficiency Division, International Energy Agency Roland Brüniger, 4E EDNA delegate for Switzerland, Swiss Federal Office of Energy 				
14h10	Presentation of the main findings from the report "Blockchain Energy Consumption - An Exploratory Study"				
	Vlad Coroama, Independent researcher, Roegen Centre for Sustainability				
14h30	Discussion and Q&A				
	Moderated by George Kamiya, Digital and Energy Analyst, International Energy Agency				
	Vlad Coroama, Independent researcher, Roegen Centre for Sustainability				
14h55	Closing				
	Pauline Henriot, 3DEN Lead Analyst, Energy Efficiency Division, International Energy Agency				
15h00	End of webinar				



Introduction to EDNA

Roland Brüniger, Swiss Federal Office of Energy (EDNA delegate for Switzerland) 12th April 2022



Introduction to EDNA

Roland Brüniger, Swiss Federal Office of Energy (EDNA delegate for Switzerland)

IEA Webinar on Blockchain Energy Consumption, 12 April 2022







Energy Implications of Device Connectivity



Energy Savings

- Digitalisation
 - Intelligent efficiency
 - Demand flexibility

Energy Cost

- Network standby
- Upstream energy





Blockchain Energy Consumption



Electronic Devices & Networks Annex

More Information

- EDNA publications and Contact
 - roland.brueniger@brueniger.swiss
 - steve@beletich.com.au

- Policy briefs
 - https://www.iea-4e.org/edna/publications/

- Swiss publications of the report
 - https://www.aramis.admin.ch/Default?DocumentID=68053&Load=true



Blockchain Energy Consumption An Exploratory Study

Vlad Coroamă

IEA Webinar, 12 April 2022

Study performed when I was still affiliated with the ETH Zurich..

ETH zürich

.. and supported to a large extent by the Swiss Federal Office of Energy



Bundesamt für Energie BFE Office fédéral de l'énergie OFEN Ufficio federale dell'energia UFE Swiss Federal Office of Energy SFOE

Energy consumption of blockchains: Topic of concern



The Big Read Bitcoin (+ Add to myFT)

Bitcoin's growing energy problem: 'It's a dirty currency'

BBC Q Home News More ▼ Q NEWS Ξ Menu

Business | Market Data | New Economy | New Tech

Tesla will no longer accept Bitcoin over climate concerns, says Musk

(§ 13 May 2021 | 🛱 Comments





Markets

Greenpeace Stops Accepting Bitcoin Donations, Cites High Energy Use

Friends of the Earth is reported to be reviewing the situation, too.

By Daniel Palmer

May 21, 2021 at 1:51 p.m.
 Updated Sep 14, 2021 at 2:59 p.m.

f in 🎔 🗳





UN News Global perspective Human stories

Search



Langua



Sustainability solution or climate calamity? The dangers and promise of cryptocurrency technology

Unsplash/André François McKenz Bitcoin is a decentralized d currency that you can buy, sell and exchange directly, without a ntermediary like a bank.

Broad consensus that energy use is growing rapidly, but variation among estimates



3

Research questions for the study

- RQ1: What are the **main drivers** of blockchain energy consumption?
- RQ2: What are likely **consumption figures** for today?
- RQ3: Are there any existing **limiting factors** and how do they act?
- RQ4: Which are effective **countermeasures**, if any?



Image source: Swiss Foundation for Technology Assessment (TA-Swiss), illustration: Hannes Saxer

Part 1: Technological Background

Why blockchains? Brief history Components of a blockchain Consensus mechanisms & proof-of-work

Technological background: Challenges of digital currencies

- Value units ('coins') of electronic currencies can be trivially multiplied, stored, and transmitted
 - (as with any digital data)
 - known as **multiple spending** problem
- Public-key-infrastructure (PKI, i.e., private-public key pair) in which all coins are signed ("**minted**") by a central Trusted Authority (TA)
 - addresses the authenticity of all original coins
 - does not solve the copying of (signed) coins and cannot prevent their multiple spending
- In first-generation digital currencies (in the 90s), TA thus required
 - not only to sign coins
 - but also to keep track (i.e., a ledger) of which accounts hold each of the coins and can rightfully spend them

Early eCash digital currency & General principles of digital currencies

- Relatively cumbersome payment in eCash
 - payer sends digital coins to payee
 - payee sends coins to TA for validation (i.e., that payer owns it, and has not used it yet for payment)
 - after validation, coins are accepted
 - TA reflects new property structure

 See also, e.g., first slide here: https://slideplayer.com/slide/10532466/

- Digital currencies
 - need a unanimously trusted ledger,
 - which can certify ownership of coins,
 - and track ownership changes.
- Drawbacks of centralised TA
 - system safety relies on TA safety (proprietary algorithms),
 - questionable scalability: TA can become bottleneck,
 - expensive and unfit for "small casual transactions", as Bitcoin was originally designed for (the irony, of course, is strong here).

Bitcoin: Digital currency based on a distributed ledger

Overall system

- Bitcoin ecosystem
 - currency units (**coins**, BTCs) & subdivisions
 - accounts that hold coins
 - transactions (either minting of new coins or transfers between accounts)
- Accounts do not directly "own" digital coins
 - as in keeping a (signed) sequence of bits on an HD
- Instead **public, distributed ledger** keeps
 - all existing account numbers (but not the owners)
 - ownership: all BTCs associated with accounts
 - all transactions ever performed

Distributed ledger

- Numerous distributed replicas of the ledger
 - held by nodes of the system
 - anyone can become a node; no access restrictions
- Can also be seen as a Virtual Machine (VM)
 - a VM state is a snapshot of accounts and coins associations
 - Bitcoin transactions represent state transitions
- Every new period (approx. 10 mins)
 - collection of transactions recorded
 - state transition occurs
 - new block of transactions added to the blockchain

- Proof of account ownership via PKI
 - private/public key pair

New issues and their solutions

Consensus mechanism

- Needed for individual nodes to agree on the valid transactions
- General problem: Decentralised nodes reaching a consensus
 - not a new problem in computer science
 - coined by later Turing-award winner Leslie
 Lamport in 1982 as 'Byzantine generals problem'
 - several solutions exist for benevolent nodes that want to reach the "correct" consensus



Sybil attack

- New solution needed for malevolent nodes
- Attacker manipulates outcome by creating a large number of nodes (pseudonyms)
 - all put forward the same result desired by the attacker
 - thus manipulating the outcome of the consensus mechanism
- In an open system w/o access restrictions
 - participation in the consensus cannot be free
 - vote needs to be bound to a limited resource coming at an expense
 - for Bitcoin (and later cryptocurrencies):
 Proof-of-Work (PoW)

Digression: One-way functions (& hashing functions)

- Functions that are "fairly easy" to compute, but almost "very hard" to revert, i.e.,
 - f(X) = Y straightforward computation
 - $f^{-1}(Y) = X$ not feasible with today's computers
- Additionally, if f(X) = Y-1, f(X+1) != Y
 - reaching "close to Y" does not help in finding Y quicker
- Thus, the only way to reach the desired outcome is by trying time and again
 - concept known in cryptography as brute force
- Thus a good PoW mechanism



10

Proof of Work (Bitcoin)



[256 bits represented by 64 hexadecimal characters]

Aim of the puzzle & work needed

- Aim: finding a result with a certain number of leading (hexadecimal) zeroes
 - amount of leading zeroes tuned so that a solution is found about every 10 minutes
 - the more nodes throw more computation at it, number will increase
- Likelihood: $1/16^{N} == 1/2^{4N}$
 - On average after $16^N == 2^{4N}$ tries (across all participating nodes)
- Currently: 20 leading zeroes
 - -2^{80} computations/hashes needed ==
 - 1'208'925'819'614'629'174'706'176 ==
 - over **1 septillion hashes** every 10 minutes

Incentivising nodes to partake in the consensus mechanism

- One-way hash function is fairly inexpensive (computationally and thus energetically)
 - it does, however, not come for free
 - and 1 septillion of them a fortiori not
- 2 types of rewards for successful node
 - transaction fees, from the accounts having transactions bundled in the new block
 - block reward from the system, newly minted BTCs

- Analogy: (search for successful nonce → new BTCs) and (digging → more gold)
 - nodes taking part thus often called miners
- Each new block links to the previous one
 - Blockchain (actually more complex Merkle tree)



Technological background recap

- To **avoid multiple spending**, a digital currency
 - needs a unanimously trusted ledger
- For scalability and open security (as opposed to security through obscurity)
 - the ledger needs to be **open** and **distributed**
- An open and distributed ledger
 - needs a **consensus mechanism** for its transactions
- The open consensus mechanism
 - is prone to **Sybil attacks** by malevolent nodes

- To counter **Sybil attacks** (i.e., through massive, pseudonymous copies)
 - a cost must be placed on the participation in the consensus mechanism
- For Bitcoin (and other currencies) the **cost**
 - is represented by the computation (work) needed to solve a cryptographic puzzle
 - (hence, such digital currencies are called cryptocurrencies)
- To **incentivise nodes** to invest these costs
 - they **receive rewards**, esp. newly mined coins

Part 2: Bitcoin Energy Consumption

Storage Communication Computation/Proof-of-work

Three sources of energy consumption for a blockchain

- *A. Storage* of the distributed VM (or distributed ledger)
- *B. Communication* among nodes, which can be triggered by some or all of the following events:
 - i. the *initial download* of the entire blockchain by a new node entering the system,
 - ii. the *transactions* submitted by individual nodes, and
 - iii. the *messages* of the consensus mechanism.
- *C. Computation* triggered by the consensus mechanism, in particular PoW (if applicable)

A. Storage energy

$$E_{St} \left[\frac{kWh}{year} \right] = \#Repl_{Av} * BC_{St} \left[GB \right] * EI_{St} \left[\frac{kWh}{year * GB} \right]$$

Term	Meaning	Value April 2022 (approx.)
#Repl _{Av}	average number of replicas (as weighted over the year)	~ 15k
BC_{St}	size of the stored blockchain (in GB)	~ 400GB
EI _{St}	average energy intensity of storing a unit of data (1 GB) for one year	0.008 – 0.66 kWh/(GB * year)

- Average energy intensity depends on the main storage medium; the two extremes being:
 - laptops/desktops dedicated exclusively: (30 W * 8760h/year) / 400GB = 0.66 kWh/(GB*year)
 - hyperscale data centres: 0.008 kWh/(GB*year)
- Range for result: 48 MWh 4 GWh energy (5.5 kW 0.45 MW average power) (worst case: yearly production of one mid-sized on-shore wind turbine)

B. Communication power

$$P_{C} = \frac{Bl [GB] * \#Repl_{Av} * (EI_{WAN} + EI_{FAN}) \left[\frac{kWh}{GB}\right]}{t [h]}$$

Term	Meaning	Value April 2022 (approx.)
Bl	size of one block of transactions	1.25 MB == 0.00125 GB
#Repl _{Av}	average number of replicas	~ 15k
EI _{WAN}	energy intensity of wide-area network	0.02 kWh/GB
EI _{WAN}	energy intensity of fixed access network	0.07 kWh/GB
t	average length of one period	600 s

- Counter of fraction represents energy to propagate a new block to all nodes
 - − 1.7 kWh/period spent all 10 minutes on average → average communication power = 10 kW
- Yearly communication energy: 88.7 MWh

C. Computational power for the PoW mechanism

- Principle: As long as the expected gain is higher than the costs, it is reasonable
 - for participants to keep mining, or
 - to freshly join the mining community
- For each miner, the (variable) mining costs for one period are



Costs per miner per period

$$C = \#H\left[\frac{hash}{period}\right] * EI_h\left[\frac{J}{hash}\right] * PUE * P_E\left[\frac{USD}{J}\right]$$

- Equation can be rewritten to reflect the state-of-the-art of mining hardware
 - as speed of hashing operations (*hash rate*)
 - for that, first term (#hashes per period) can be expressed as:

$$C = t[s] * HR \left[\frac{hash}{s}\right] * EI_h \left[\frac{J}{hash}\right] * PUE * P_E \left[\frac{USD}{J}\right]$$

length of period hash rate (hashes per second)

Expected revenue per miner per period

• Expected revenue equals the likelihood for miner to be successful times the total reward for successful mining



System equilibrium when expected revenue equals costs E(R) == C

$$t * HR * EI_h * PUE * P_E = \frac{t * HR}{2^{4N}} * (\#CC * P_{CC} + T)$$

• Can be simplified to

$$EI_h * PUE * P_E = \frac{(\#CC * P_{CC}) + T}{2^{4N}}$$

• The equilibrium energy intensity of a hashing operation can be derived by solving the identity:

$$EI_h = \frac{1}{2^{4N}} * \frac{(\#CC * P_{CC}) + T}{P_E * PUE}$$

- unsurprisingly, directly correlated to the reward expected, $(\#CC * P_{CC}) + T$
 - and thus essentially to the price of the cryptocurrency, P_{CC}
- inversely related to what makes mining more expensive
 - the (average) price of electricity P_E as well as the *PUE*, which stands for the "wasted" share of electricity
 - the **complexity of the cryptographic puzzle** (and thus the needed amount of hashing operations)

Deriving an upper bound for WW electricity consumption of PoW

• Using the EI_h estimate to compute an upper bound for the WW electricity consumption of PoW per block/period:

$$E_{PoW}(WW, one \ period) \left[\frac{J}{period} \right] = \#H \left[\frac{hash}{period} \right] * EI_h \left[\frac{J}{hash} \right] * PUE$$

- Knowing
 - the expected number of hashes during one period $#H = 2^{4N}$, and
 - dividing by the average length of one period t,

yields an upper-bound for the WW power consumption used for PoW:

$$P_{PoW}(WW) = \frac{2^{4N} * EI_h * PUE}{t}$$

• Using the equilibrium (i.e., threshold) energy intensity EI_h as computed above, yields $P_{PoW} = \frac{2^{4N} * PUE}{t} * EI_h = \frac{2^{4N} * PUE}{t} * \frac{1}{2^{4N}} * \frac{(\#CC * P_{CC}) + T}{P_E * PUE} = \frac{(\#CC * P_{CC}) + T}{t * P_E}$

Upper bound for WW electricity consumption of PoW

$$P_{PoW}(WW) = \frac{(\#CC * P_{CC}) + T}{t * P_E}$$

- Current Bitcoin data:
 - $\#CC = 6.25 * P_{CC} \sim 40k \ USD = 250k \ USD, T \sim 1500 \ \text{transactions} * 2 \frac{\text{USD}}{\text{transaction}} = 3,000 \ \text{USD}$ (reward is thus around 250,000 USD)

$$-t = 600s, P_E = \frac{0.05USD}{kWh}$$
$$P_{PoW}(WW) = \frac{250,000 USD}{600 \ s * 0.05 \frac{USD}{kWh}} = \frac{250,000 \ kWh}{30 \ s}$$

• Given that 1 kWh = 3,600 "kWs", this results in

$$P_{PoW}(WW) = \frac{250,000 * 3,600}{30} \frac{kWs}{s} = (250,000 * 120) kW = 30 \, GW$$

Interpretation of PoW power and energy

• Worst case WW power and yearly energy:

$$P_{PoW}(WW) = 30 \; GW; \; E_{PoW}(WW) = 263 \frac{TWh}{year}$$

- This worst-case figure amounts to
 - power production of 30 nuclear power plants
 - yearly electricity consumption of ~Spain, Australia, UK (top 11-20 WW)
 - almost Romania's entire (i.e., primary) energy consumption (370 TWh/year), and slightly more than Portugal's (259 TWh/year)
 - similar to the entire energy consumption of all (non-crypto) data centres WW: 200 400 TWh/year (Masanet et al. 2020 and Borderstep 2019, respectively)
 - around 1% of WW electricity usage

Comparison to related work (all TWh/year)

Period	Publication	Date	Lower bound	Expected	Upper bound
	(de Vries 2018)	May-18	22	67	78
	(Krause and Tolaymat 2018)	Nov-18		30	
Earlier studies	(Stoll et al. 2019)	Jul-19		46	
	(de Vries 2020)	Sep-19		87	
	(Bendiksen and Gibbons 2019)	Dec-19		61	
	(Sedlmeir et al. 2020)	Feb-20	60		125
	(Cambridge BECI 2021)	Apr-22	54	144	362
Current studies	(Digiconomist 2021)	Apr-22	61	204	
	this study	Apr-22			263

Part 3: Getting to Grips with the Consumption

Natural limiting mechanisms? Governmental and private policies Weighting against benefits

Individual consumption for Blockchain components



How does this appear on linear (non-logarithmic) scales?



Mechanisms limiting the energy consumption of PoW?



- Value entirely determined by
 - rewards value (mined coins and transaction fees) & price of electricity
- No economic counteracting mechanism
 - except, perhaps, indirectly (and very slowly) over an increasing electricity price
- No technological mechanisms either: Entirely independent of mining hardware efficiency
 - in the short run, more efficient HW represents competitive advantage, can pull total down from worst-case
 - in the long run, everyone switches to the more efficient HW, pushing total again towards worst-case
 - typical rebound effect (unfortunately, not the topic here, but essential concept in the context of digital efficiency)

Alternative consensus mechanisms

- Several alternative consensus mechanisms, chief among them "Proof-of-Stake" (PoS)
 - getting rid of the concept of miners entirely
 - owing blockchain's native cryptocurrency enables one to be validator
- Validators for each block randomly chosen
 - likelihood to be chosen proportional to stake
 - return on investment 2 18% of stake/year
 - Sybil attack would require >50% of stake
- Some cryptocurrencies already deploy PoS
 - e.g., EOS, Tezos, TRON
 - Ethereum is changing towards it (Eth. 2.0)

Platform	Global (kW)		Per transaction (kW h/tx)		
Eth. 2.0 [↑]	1010.6 -	30 887.5	0.000 09 -	0.002 86	
Eth. 2.0↓	1010.6 -	30887.5	0.018 23 -	0.557 13	
Algorand	6.2 –	189.3	0.00017 -	0.005 34	
Cardano	16.3 –	497.2	0.01239 -	0.378 54	
Polkadot	1.6 –	49.9	0.00378 -	0.115 56	
Tezos	2.2 -	67.1	0.000 36 -	0.01096	
Hedera	3.5 -	6.9	0.000 02 -	0.000 04	
Bitcoin	3 373 287.7 - 34	4817351.6	360.393 00 - 3	691.407 00	
VisaNet	X	22 387.1		0.003 58	
[↑] High throughput projection ↓ Low throughput projection					
consensus mechanism needs a factor of 1000-3000 less energy, once PoS implemented (for similarly-sized blockchains)					

30

The most efficient policy interventions are those discouraging/banning PoW-based blockchains

Not only public policies, btw; companies have power (and thus responsibility) as well

euronews.next

Europe rejects proposal limiting PoW cryptos such as Bitcoin but sets draft rules for sustainability

By Pascale Davies • 14/03/2022



Several EU parliamentarians have been pushing to ban PoW cryptos over energy concerns - Copyright CANVA

The European Union has rejected a proposed rule that could have banned the cryptocurrency Bitcoin across the bloc but set new draft rules to protect consumers and make mining more sustainable.

How Elon Musk's tweets have moved bitcoin prices



Blockchain benefits - investment & inflation hedging

Cryptocurrency: Hedge against inflation



NFTs on digital & physical assets

Neue Zürcher Zeitung

Schweizer Bank digitalisiert Meisterwerk: Ein Stück Picasso ins Portfolio legen

Die Sygnum Bank ermöglicht den fraktionalen Kauf eines Gemäldes des spanischen Meisters. Damit eröffnet das Schweizer Institut einen ungewöhnlichen Zugang zu einer neuen Anlageklasse.

"Swiss bank digitalises masterpiece – put a piece of Picasso in your portfolio."

Werner Grundlehner 15.07.2021, 09.41 Uhr

 \equiv



Blockchain benefits: Smart contracts & DeFi for development

Towards a Blockchain Special Purpose Vehicle for Financing Independent Renewable Electricity Projects in Sub-Saharan Africa

Olakunle Alao, Member, IEEE and Paul Cuffe, Member, IEEE



33

0&A



Schweizerische Eidgenossenschaft Confédération suisse Confederazione Svizzera Confederaziun svizra Federal Department of the Environment, Transport, Energy and Communications DETEC

Swiss Federal Office of Energy SFOE Energy Research and Cleantech Division

Final report dated 27 September 2021

Blockchain energy consumption

An exploratory study

Full study: https://www.aramis.admin.ch/Default?DocumentID=68053