Inventemos Web4 porque…
Web3 apesta.

😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱

Santiago Saavedra - esLib.re 2022 · Sala de Privacidad y Soberanía Digital

Cómo hemos llegado hasta aquí?

NUMBER GO UP
HODL
BULLISH
TO THE MOON

Blockchain: dos tecnologías

Permissioned

- Establecido en 1990
- Confianza entre nodos implícita
- Protocolos eficientes, como BFT (Byzantine Fault Tolerance) [paper]
- Mecanismo de ***consenso*** para sistemas distribuidos

Permission-less

- Establecido en 2008
- Cada participante resuelve un cálculo diferente para llegar a un estado *diferente* de la cadena, determinado por un mecanismo de ***decisión***.
- No hay autoridad central
- Sybil attacks

Economía 101

Permissionless blockchains

- No hay autoridad central
  - Sybil attacks
- Garantizar que recompensa(éxito) < coste(setup)
  - Por lo tanto, participar **necesita ser caro**
    - Parte del proceso: mineros *necesitan* recuperar sus costes
- **Necesita una criptomoneda** como incentivo económico para garantizar la seguridad de la información

Economía 102

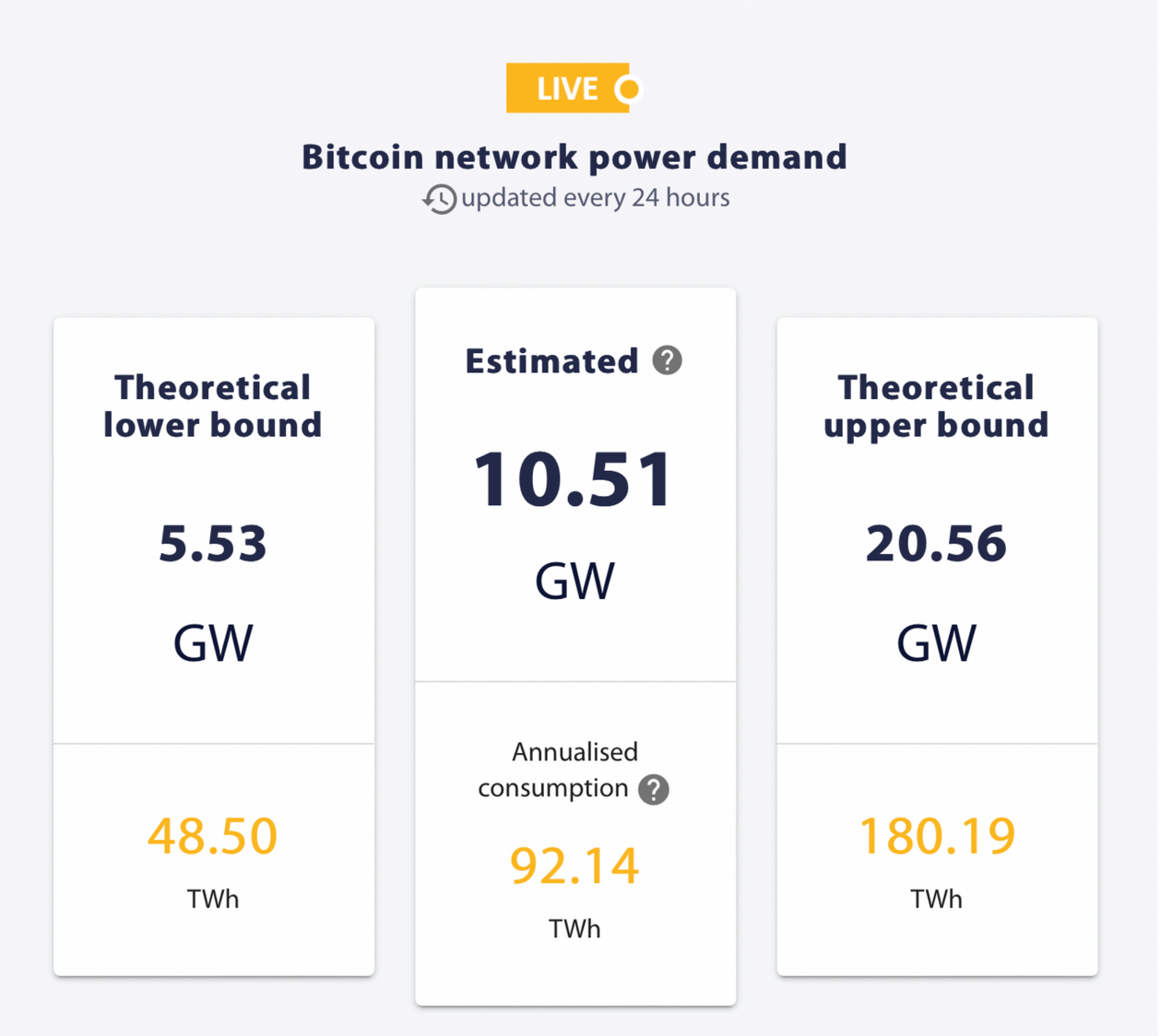
Permissionless blockchains

- **Necesita una criptomoneda** como incentivo económico para garantizar la seguridad de la información
- Hay que pagar los costes mineros
  - Recordemos: **tiene que ser caro** ser minero para garantizar la seguridad
- Mineros no pueden pagar sus costes (capex, opex) en la criptomoneda
  - Mineros tienen que vender cripto para pagar sus costes.
  - Alguien tiene que comprar. ¿Cuál es la razón para comprar?
    - NUMBER GO UP

Una blockchain permissionless:

necesita una criptomoneda para funcionar, y esta criptomoneda **necesita de la especulación** para funcionar.

Consumo energético



Fuente: https://ccaf.io/cbeci/index

The waste

Fuente: Pixabay, https://pixabay.com/es/photos/garbage-la-contaminación-dump-4857295/
Licencia: Pixabay License

Bitcoin e-waste
=
Netherlands e-waste

Fuente: https://doi.org/10.1016/j.resconrec.2021.105901

Usar y tirar

ASIC

=

“Application Specific Integrated Circuit”

1,25 años

Duración media de un ASIC de minado de Bitcoin antes de convertirse en e-waste

Fuente: https://doi.org/10.1016/j.resconrec.2021.105901

Emisiones

Scope 3

- La mayor parte de emisiones en centros de datos vienen de:
la cadena de suministro

Emisiones de CapEx > OpEx

- Fuente: https://arxiv.org/pdf/2011.02839.pdf

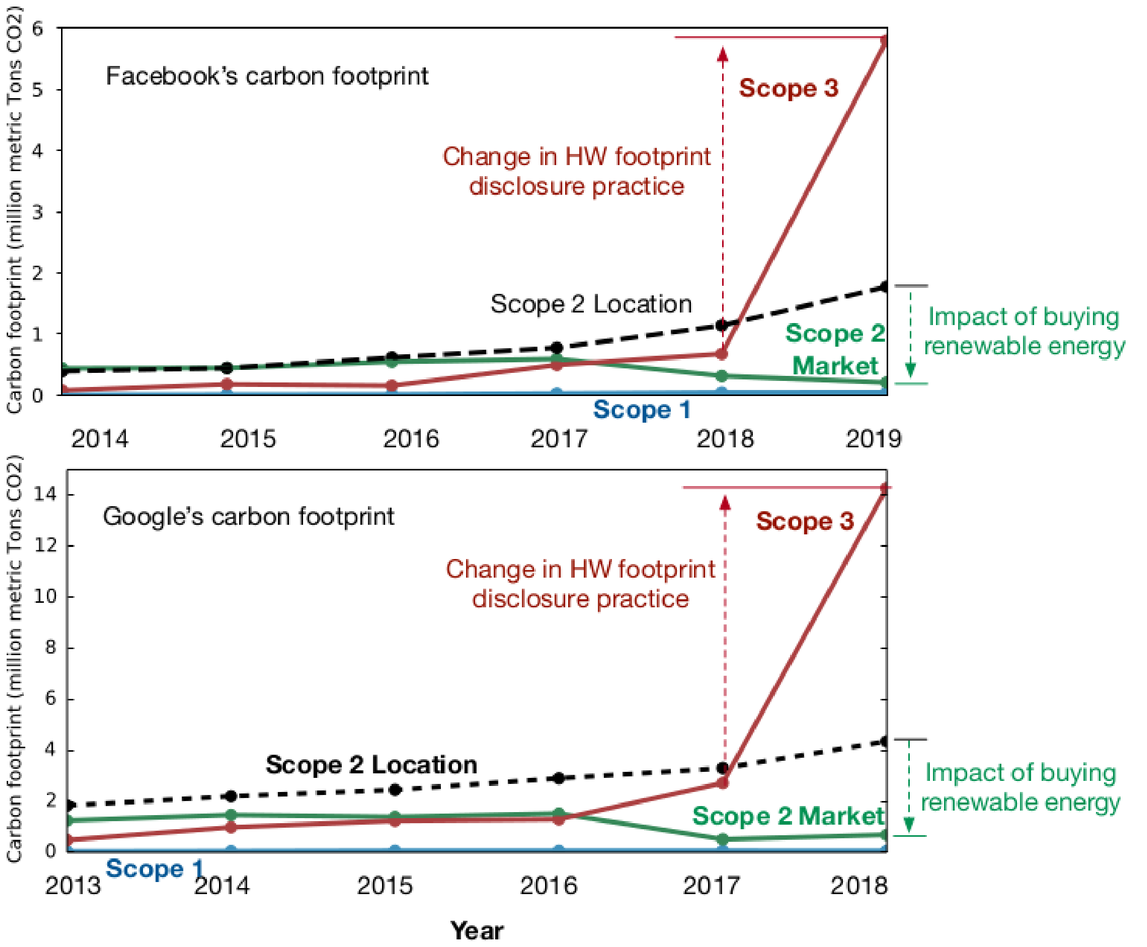


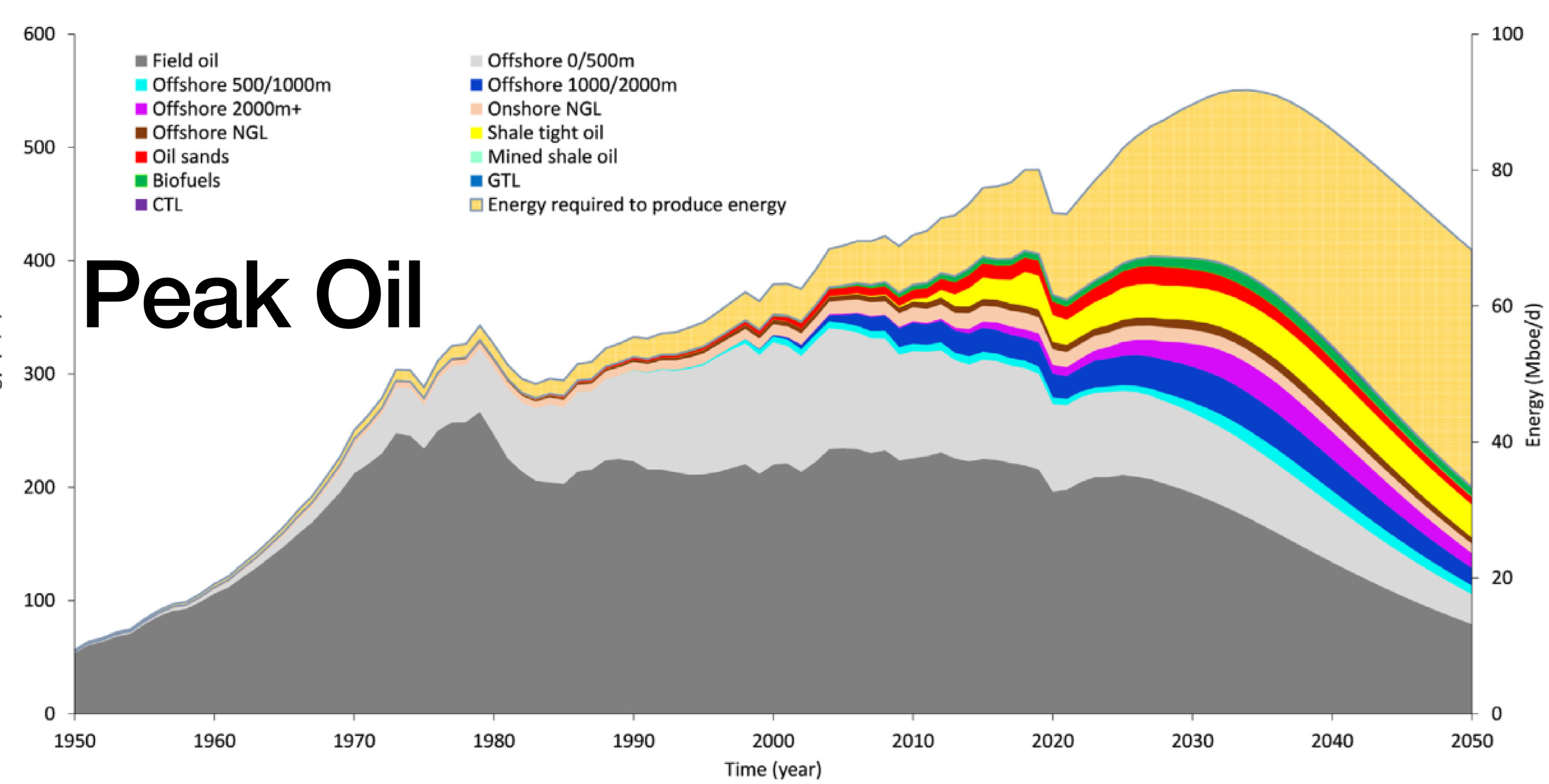
Fig. 11. Carbon footprint of Facebook and Google (two large data center operators). As data centers increasingly rely on renewable energy, carbon emissions originate more from Scope 3, or supply-chain emissions (e.g., hardware manufacturing and construction).

Emisiones
“Verdes”

"We have been long-time believers in the importance of sustainable cryptocurrency operations," said Ken MacLean , President of the LUXX Mining Division, which operates an industrial-scale cryptocurrency mining operation in New Mexico . "Through our partnership with the Navajo Tribal Utility Authority ("NTUA"), we are able to access some of the most affordable and environmentally friendly energy in the world. We look forward to expanding that partnership as members of the Crypto Climate Accord, and we encourage crypto companies everywhere to consider how they can operate as sustainably as possible."

Crypto miner Luxxfolio has signed up to the Crypto Climate Accord “committing” them to power all their mining with 100% renewable electricity. How are they implementing this? By buying 15 megawatts of coal-fired power from the Navajo Nation! They’re paying less than a tenth what other Navajo pay for their power — and 14,000 Navajo don’t have *any* access to electricity. The local Navajo are not happy. [*press release*; *Facebook*]

- Fuentes:
  - https://money.tmx.com/en/quote/LUXX:CHI/news/5718111260601144/LUXXFOLIO_signs_Crypto_Climate_Accord_reflecting_commitment_to_green_cryptocurrency_mining_and_exchange
  - https://davidgerard.co.uk/blockchain/2021/09/21/news-bitcoin-miners-cant-sell-their-bitcoins-sushiswap-theft-coinbase-lend-crypto-seasteading/

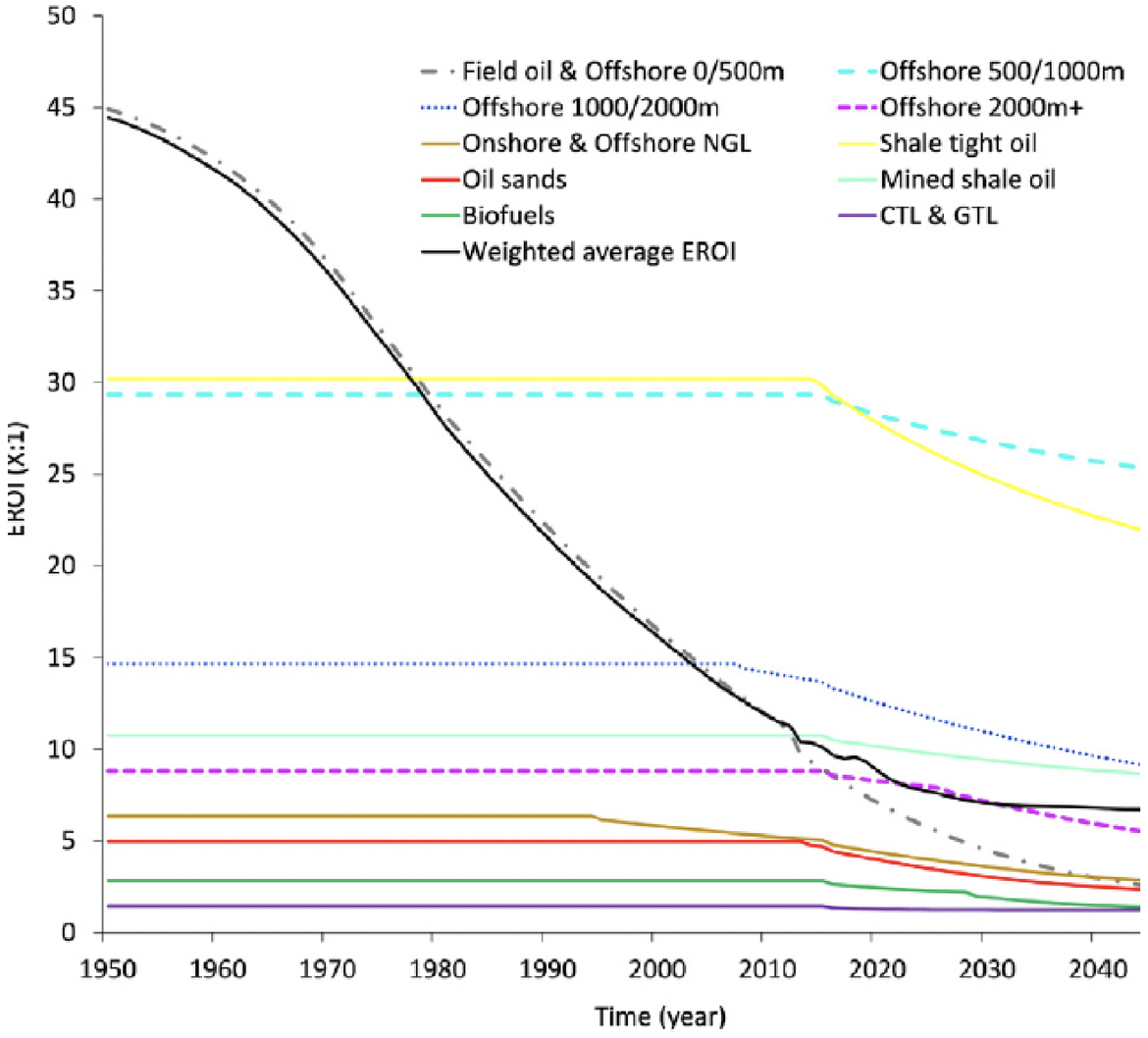


Fuente: https://doi.org/10.1016/j.apenergy.2021.117843

Fig. 1. Average oil liquids net-energy production from 1950 to 2050, compared to the gross energy.

La energía cuesta energía

Y ya no nos podemos permitir desperdiciarla

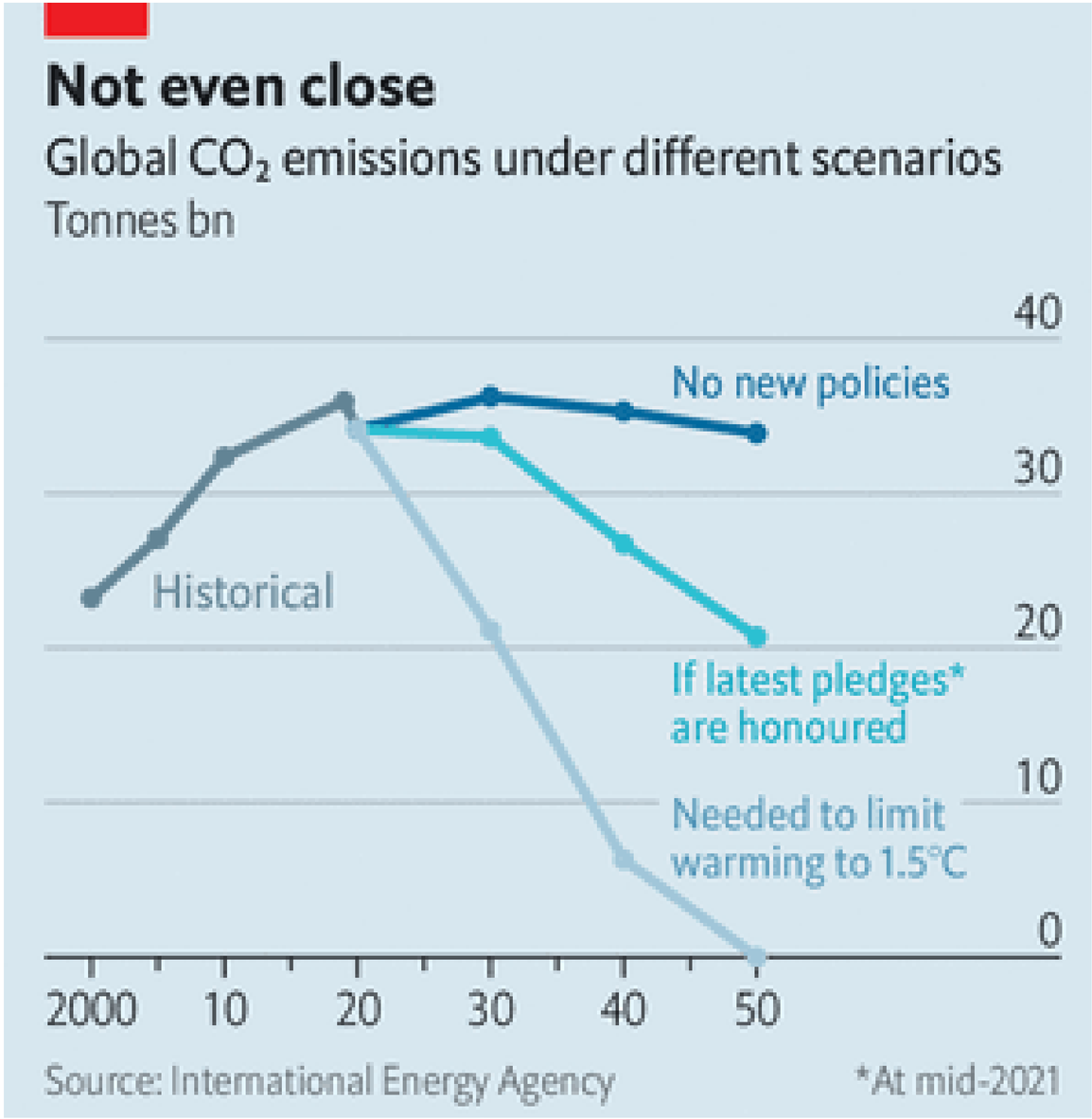


Fuente: https://doi.org/10.1016/j.apenergy.2021.117843 (Fig. 2)

Perspectivas de CO2

Vamos mal

- La transición energética requiere energía
- Desplegar renovables requiere gastar energía para producir equipamiento
- Tenemos que reservar esa energía y no desperdiciarla



Chia

Y si usamos espacio de almacenamiento como prueba en lugar de poder de cómputo? (Proof-of-storage)

“We've kind of destroyed the short-term supply chain”

Gene Hoffman, presidente de la Chia Network

Fuente: https://www.newscientist.com/article/2278696-bitcoin-rival-chia-destroyed-hard-disc-supply-chains-says-its-boss/

Proof of Stake

¿La solución?

El coste de la apuesta (stake) es hacer la participación cara a riesgo de pérdida del capital y de la liquidez mientras está apostada.

- Desigualdad auto-reforzante
- Number go up

HOME > MARKETS

How Bitcoin Is Like North Korea

Joe Weisenthal Jan 12, 2014, 5:04 PM

Best estimates are that there are about one million holders of Bitcoin; 47 individuals hold about 30 percent, another 900 hold a further 20 percent, the next 10,000 about 25% and another million about 20%, with 5% being lost. So 1/10th of one percent represent about half the holdings of Bitcoin and 1 percent close to 80 percent (http://www.businessinsider.com/927-people-own-half-of-the-bitcoins-2013-12). The concentration of Litecoin ownership is similar (http://litecoin-rich-list.blogspot.com). Most of the big wallets have been in place from early on, so sitting back and watching your capital grow has been a very successful strategy.

90% of transaction volume on the Bitcoin blockchain is **not** tied to **economically meaningful** activities but is the byproduct of the Bitcoin protocol design as well as the preference of many participants for anonymity. … exchanges play a central role in the Bitcoin system. They explain 75% of real Bitcoin volume … Our results do not support the idea that the high valuation of cryptocurrencies is based on the demand from illegal transactions. Instead, they suggest that the majority of Bitcoin transactions is linked to speculation.

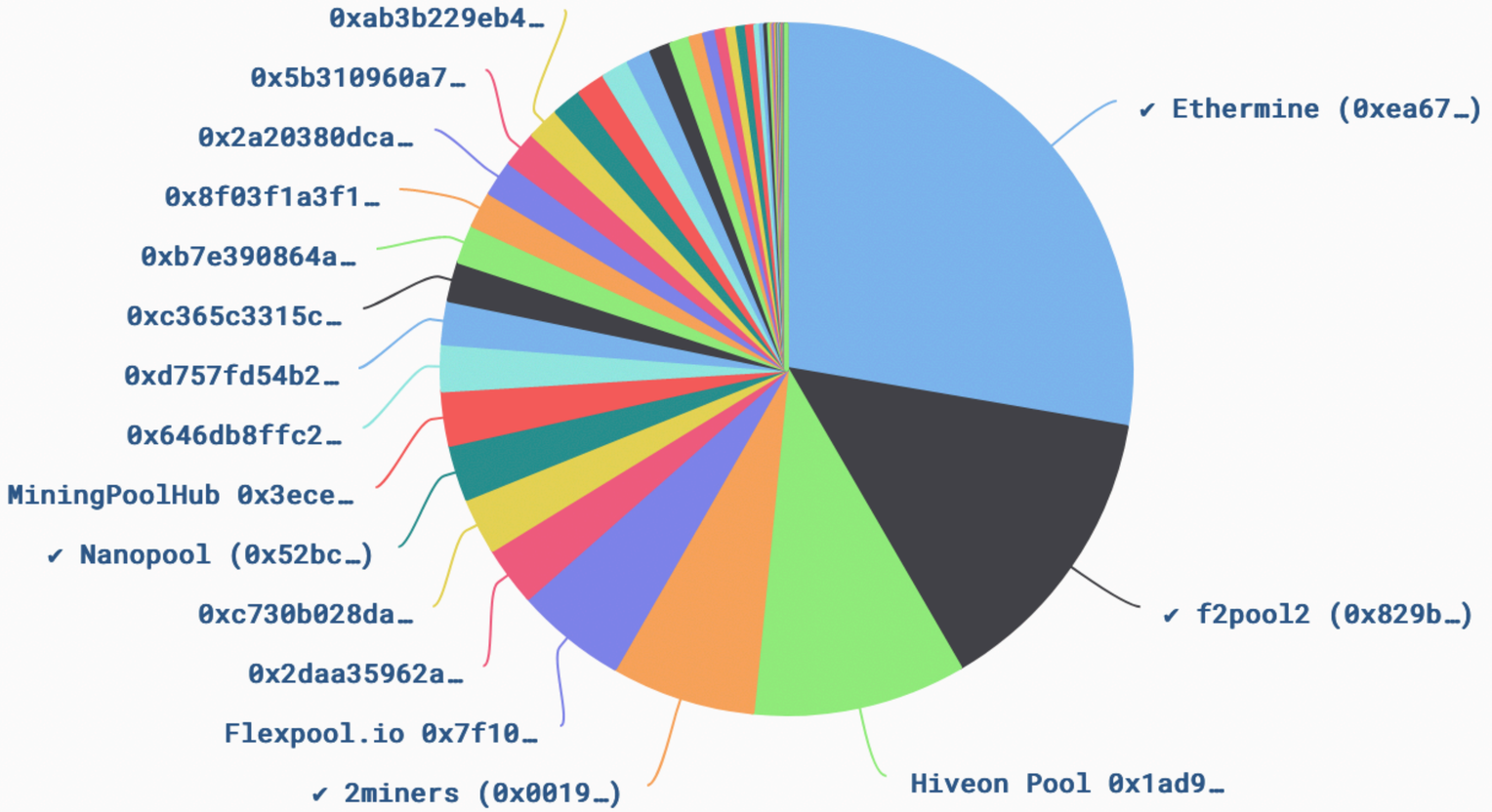
Makarov and Schoar, **Blockchain Analysis of the Bitcoin Market**


Transacciones
350k
300k
250k
200k
Blockchain.com
2020
2021
2022


NYPD

Descentraliación? No tanto!

3 Pools > 50% ETH



Fuente: https://www.etherchain.org/miner

Anti blanqueo de capitales?
(Nope)

"There's a certain amount of Bitcoin politics involved here. On the one hand you have groups in the bitcoin community who are all about maximum decentralization. They are against the whole concept of doing anything that has to do with financial regulatory compliance or government regulation. Then there are the institutional investors who like the fact that people are trying to make the blockchain more compliant because it makes it safer for you to invest."

Fuente: https://miningpoolstats.stream/ethereum

“First, non-KYC entities serve as a gateway for money laundering and other gray activities. […]

Second, even if KYC entities were restricted to deal exclusively with other KYC entities, preventing inflows of tainted funds would still be nearly impossible, unless one was willing to put severe restrictions on who can transact with whom […]

Finally, notice that while transacting in cash and storing cash involve substantial costs and operational risks, transacting in cryptocurrencies and storing them are essentially costless (apart from fluctuation in value).”

Igor Makarov & Antoinette Schoar, National Bureau of Economic Reserach (DOI 10.3386/w29396)

Fuente: https://www.nber.org/papers/w29396

The singular reason why these attacks are even possible is due entirely to rise of cryptocurrency. Consider the same situation on top of the existing international banking system. **Go to your local bank branch and try to wire transfer $200,000 to an anonymous stranger in Russia and see how that works out.** Modern ransomware could not exist without Bitcoin, it has poured gasoline on a fire we may not be able to put out.

When you create a loophole channel (however flawed) for parties to engage in illicit financing of anonymous entities beyond the control of law enforcement, it turns out a lot of shady businesses models that are otherwise prevented move from being impractical and risky to perversely incentivized. Ransomware is now very lucrative to the point where there is a whole secondary market of vendors selling Ransomware as a Service picks and shovels to the criminals.

Stephen Diehl

Fuente: https://www.stephendiehl.com/blog/ransomware.html

“90% of transaction volume on the Bitcoin blockchain is not tied to economically meaningful activities but is the byproduct of the Bitcoin protocol design as well as the preference of many participants for anonymity.”

Igor Makarov & Antoinette Schoar, Blockchain Analysis of the Bitcoin Market (DOI 10.3386/w29396)

Fuente: https://www.nber.org/papers/w29396

Inmutabilidad: smart contracts

Y el crimen…

DeFi100 - Rebase

WE SCAMMED YOU GUYS AND YOU CANT DO SHIT ABOUT IT

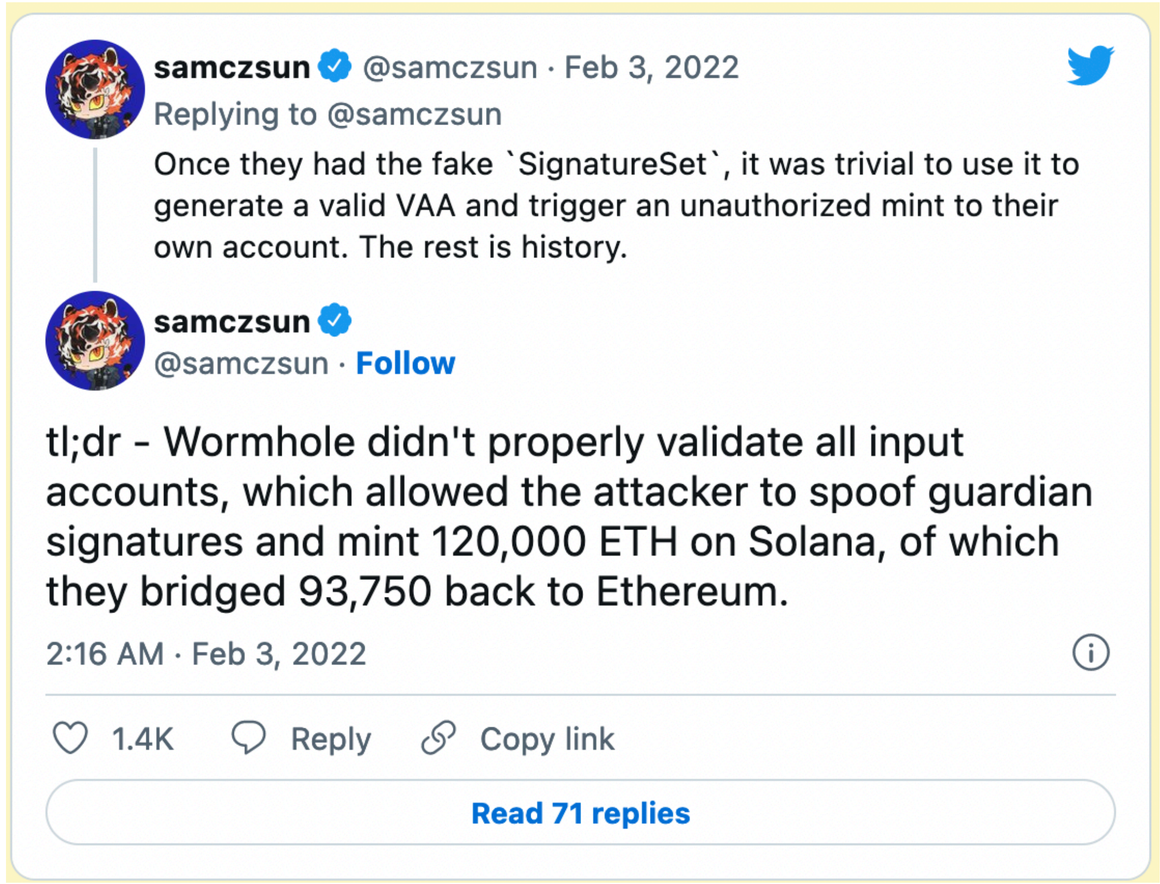
HA HA.. All you moon bois have been scammed and you cant do shit about it - DEVSIN

Guante blanco

FUCK YOU MOONBOIS

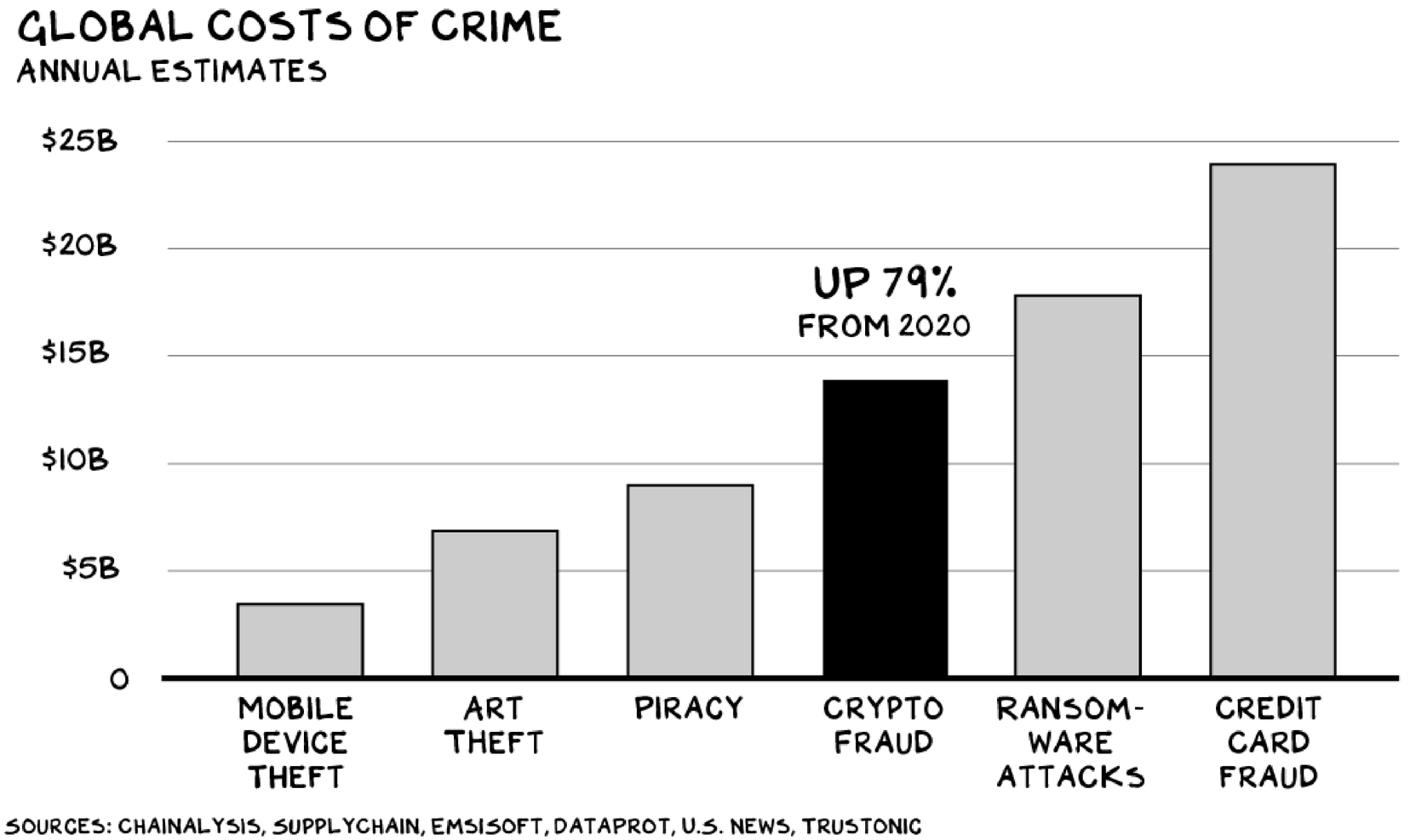
Ejemplos

- Cream finance ($38M, $19M y $130M)
- BadgerDAO ($115M)
- BitMart ($196M)
- Wormhole ($323M)
- Poly Network ($600M)



Y el crimen…

Si estamos en contra de AML/KYC…



Y el crimen…

Si estamos en contra de AML/KYC…

La economía

jack⚡
@jack

You don't own "web3."

The VCs and their LPs do. It will never escape their incentives. It's ultimately a centralized entity with a different label.

Know what you're getting into...

¿Qué es Web3?

O.. que dicen ellos?

"Web3 is a decentralized version of the internet where platforms and apps are built and owned by users. Unlike web2 (the current web), which is dominated by centralized platforms such as Google, Apple, and Facebook, web3 will use blockchain, crypto, and NFTs to transfer power back to the internet community."

¿Qué es Web3?

Bueno, a ver.

"Web3 is a decentralized version of the internet where platforms and apps are built and owned by ~~users~~ corporations who aspire to be just like~~. Unlike web2 (the current web), which is dominated by centralized platforms such as~~ Google, Apple, and Facebook, ~~web3 will use~~ but using fancy new words like blockchain, crypto, and NFTs to make the impression that they are transferring power back to the internet community."

¿Qué es Web3?

Bueno, a ver.

Arreglado!

"Web3 is a version of the internet centralized around ledgers where platforms and apps are built and owned by corporations who aspire to be the new Google, Apple, and Facebook, but using fancy new words like blockchain, crypto, and NFTs to make the impression that they are transferring power back to the internet community while in fact they are mostly increasing inequality."

Narrativa

Lo bueno

Abajo las grandes empresas!

Abajo los intermediarios

Las reglas claras

Narrativa

Lo feo

Abajo las grandes empresas (queremos ser nosotros)!

Abajo los intermediarios (en realidad los necesitamos también)

Las reglas claras (más bien no renegociables)

Narrativa

Lo malo

Abajo las grandes empresas (queremos ser nosotros, ¡y desregulados!)!

Abajo los intermediarios (en realidad los necesitamos también…

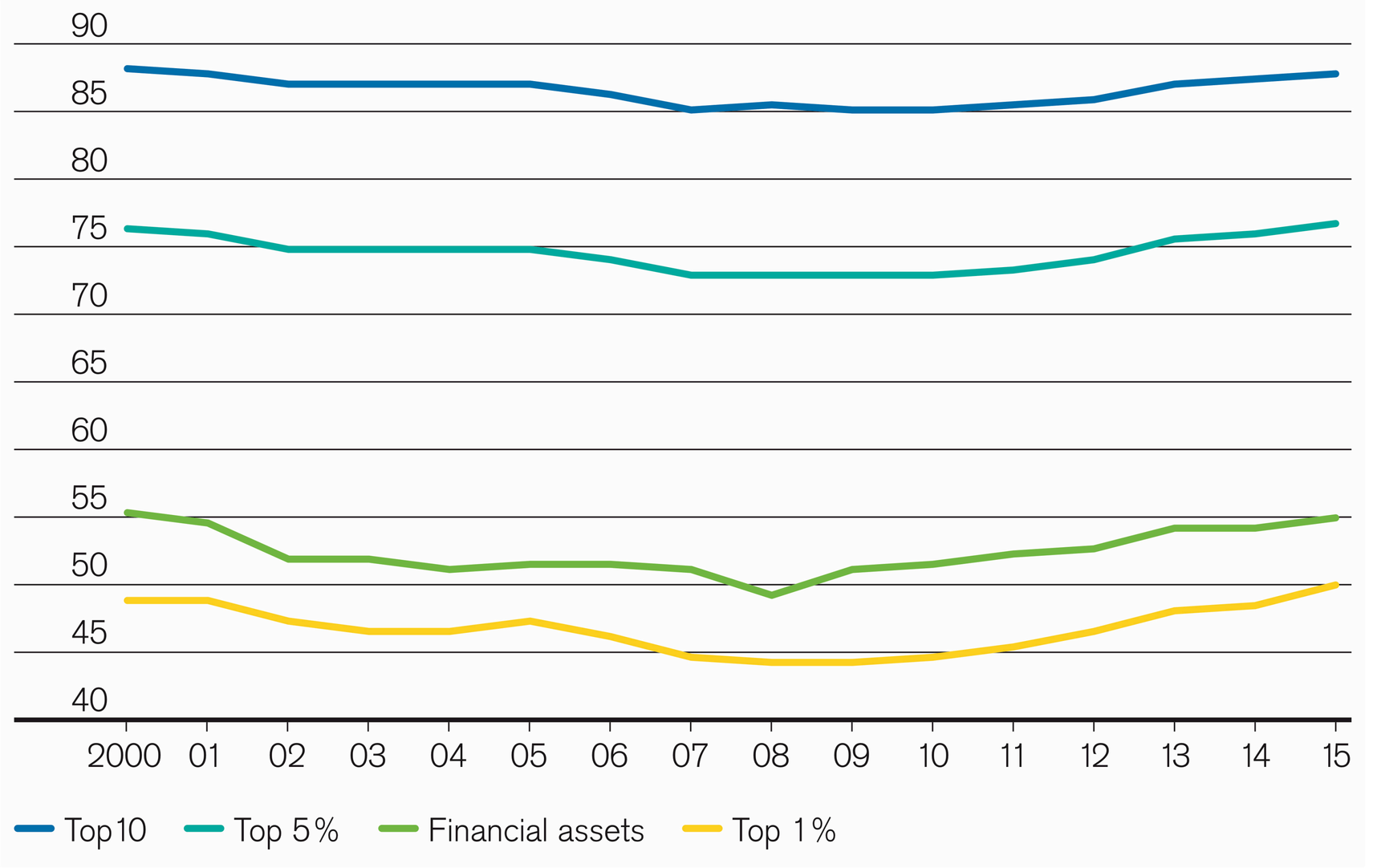
¡y no quieren respetar la legislación!)

Las reglas ~~claras~~ invariantes, a menos que tengas mucho poder ☝️

Es que la desigualdad económica…

Figure 6

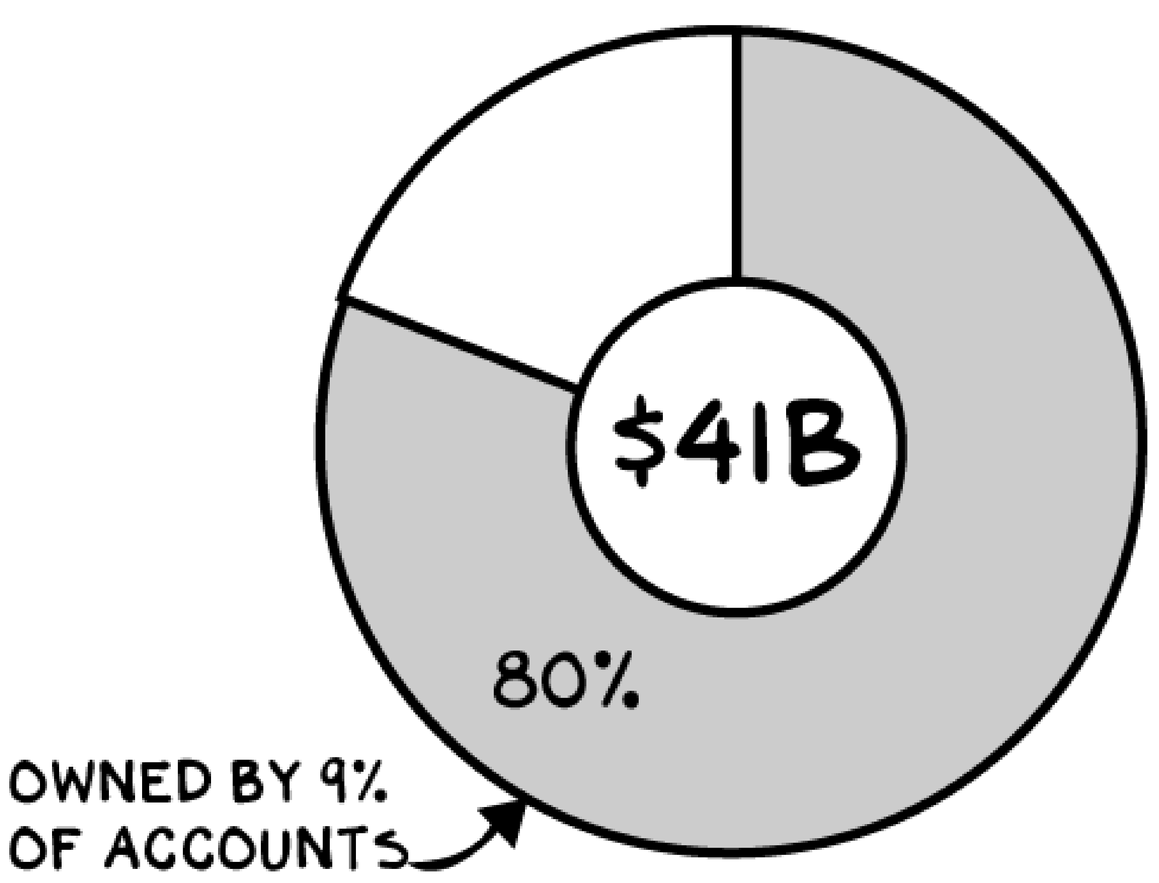
Share of top wealth holders and share of financial assets (%), 2000–2015



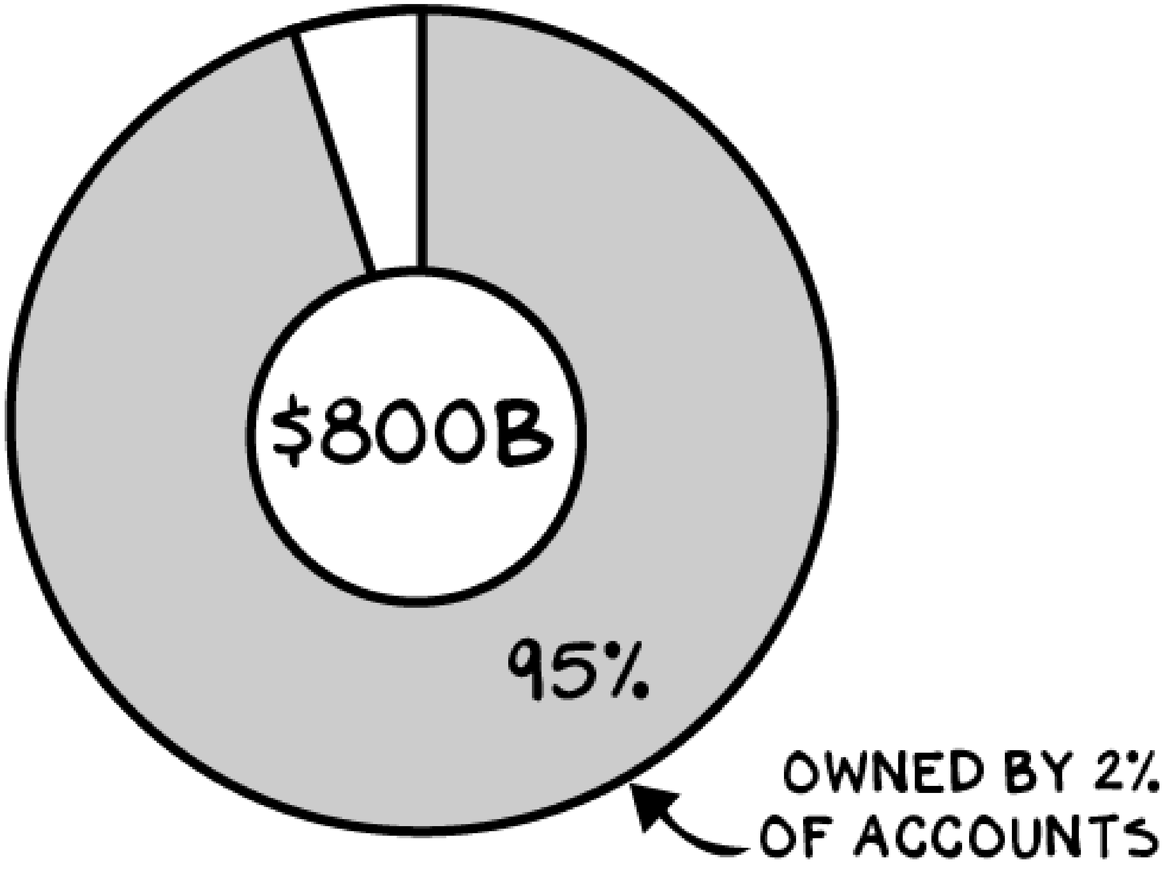
Source: James Davies, Rodrigo Lluberas and Anthony Shorrocks, Credit Suisse Global Wealth Databook 2015

INEQUALITY IN CRYPTO

2021



NFT MARKET



BITCOIN

SOURCES: CHAINALYSIS, FLIPSIDE CRYPTO NOTE: NFT MARKET=NFTS ON ETHEREUM BLOCKCHAIN NETWORK.

2% de las cuentas

95% del volumen de la divisa

Fuente: https://bitinfocharts.com/top-100-richest-bitcoin-addresses.html

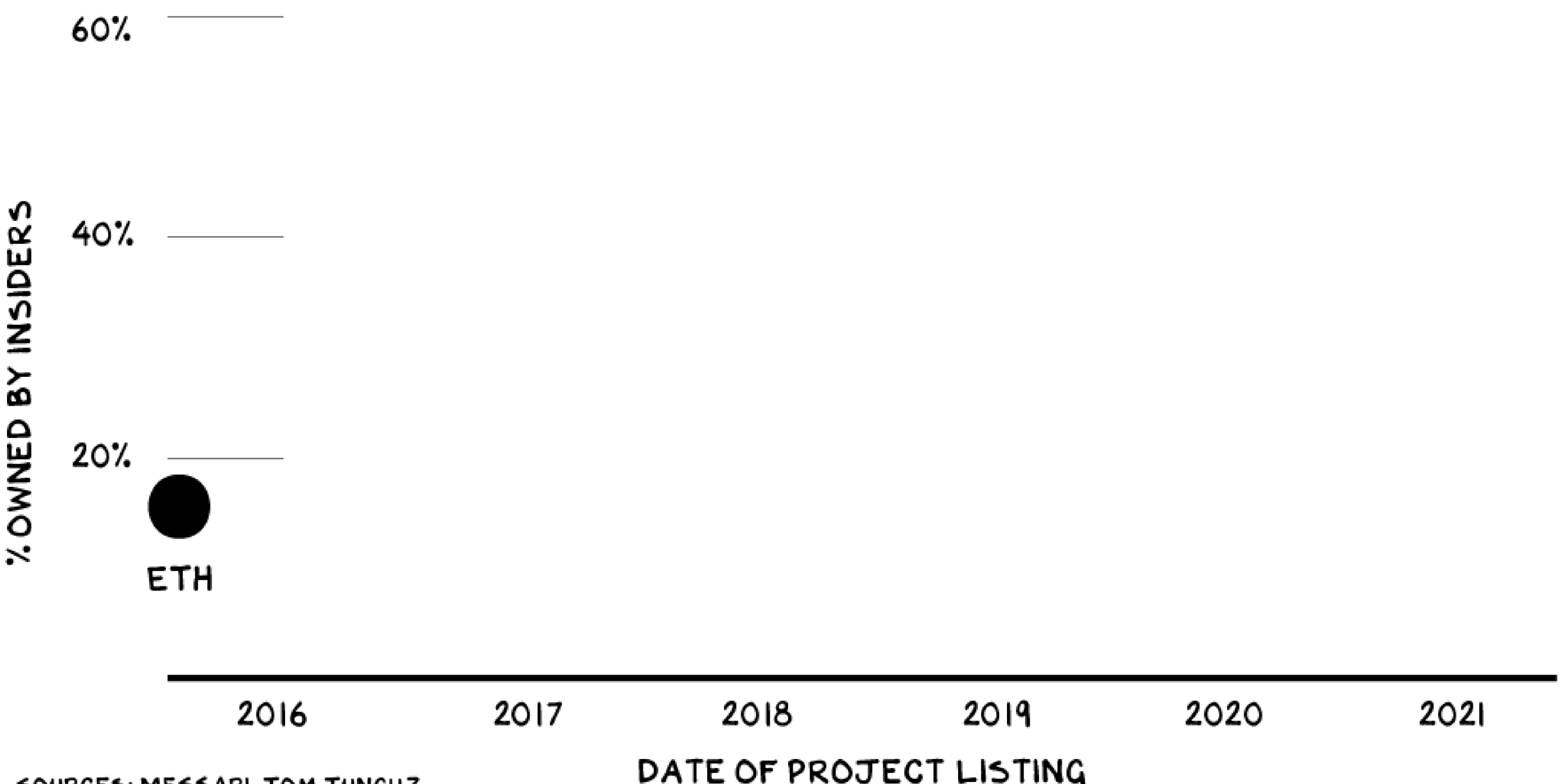
0.1%

de los mineros suponen el 50% de la potencia de minado

Fuente: https://www.techspot.com/news/91937-bitcoin-largely-controlled-small-group-investors-miners-study.html


Inside ownership
stonks

CRYPTO PROJECTS: INSIDER OWNERSHIP SHARE AT LAUNCH

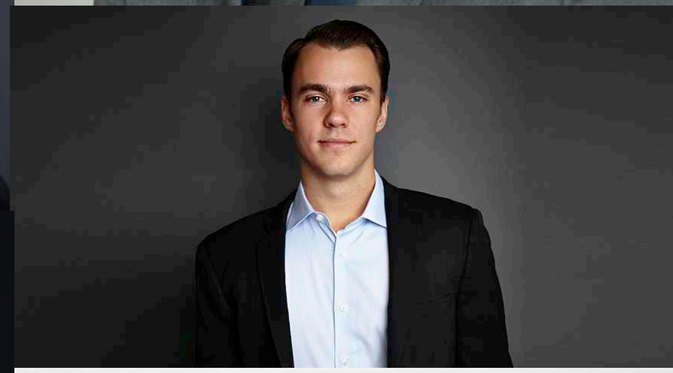
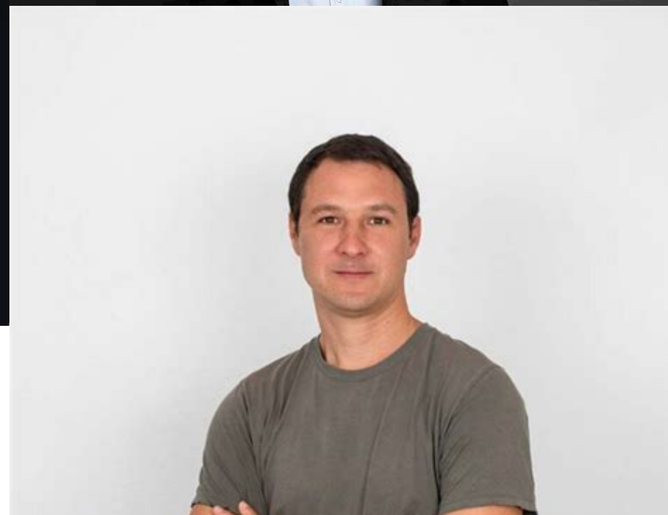


SOURCES: MESSARI, TOM TUNGUZ

Forbes 2021 Cryptobillionaires

Fuente: https://www.forbes.com/sites/johnnyatt/2021/04/06/the-cryptocurrency-tycoons-on-forbes-2021-billionaires-list/





Fuente: https://www.forbes.com/sites/johnnyatt/2021/04/06/the-cryptocurrency-tycoons-on-forbes-2021-billionaires-list/

Los intermediarios…

INFURA

PRODUCTS USE CASES PRICING DOCS RESOURCES EN SIGN UP LOGIN

Blockchain as a Service?

¿Podría ser más obvio?

The World's Most Powerful Blockchain Development Suite

Our suite of high availability APIs and Developer Tools provide quick, reliable access to the Ethereum and IPFS networks so you can focus on building and scaling next generation software.

Log in to your dashboard

Email

Password

LOG IN

OR

New to Infura? Get started for free.

SIGN UP

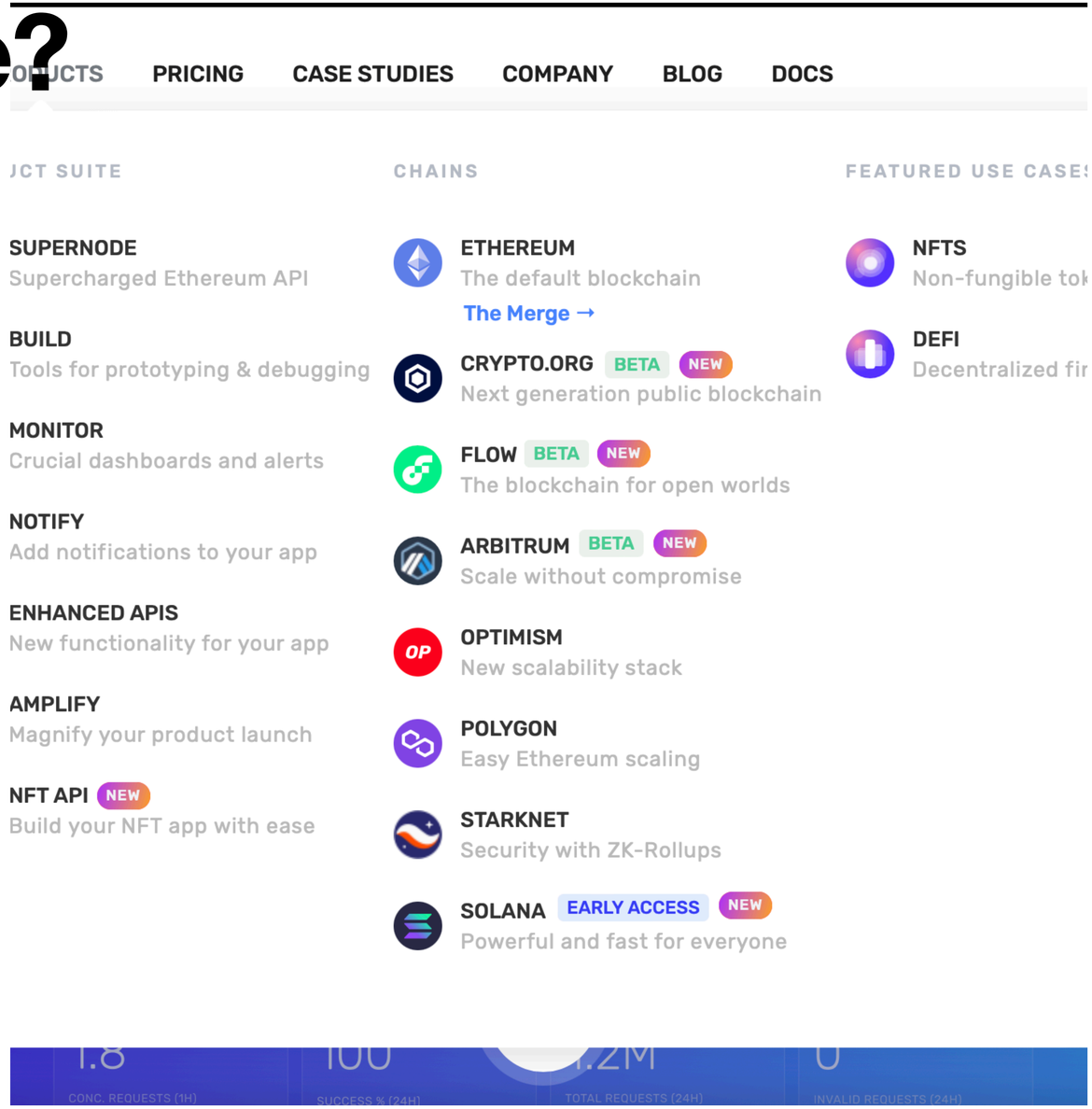
Brought to you by

Need a custom solution? Contact us

Blockchain as a Service?

Blockchain as a Service

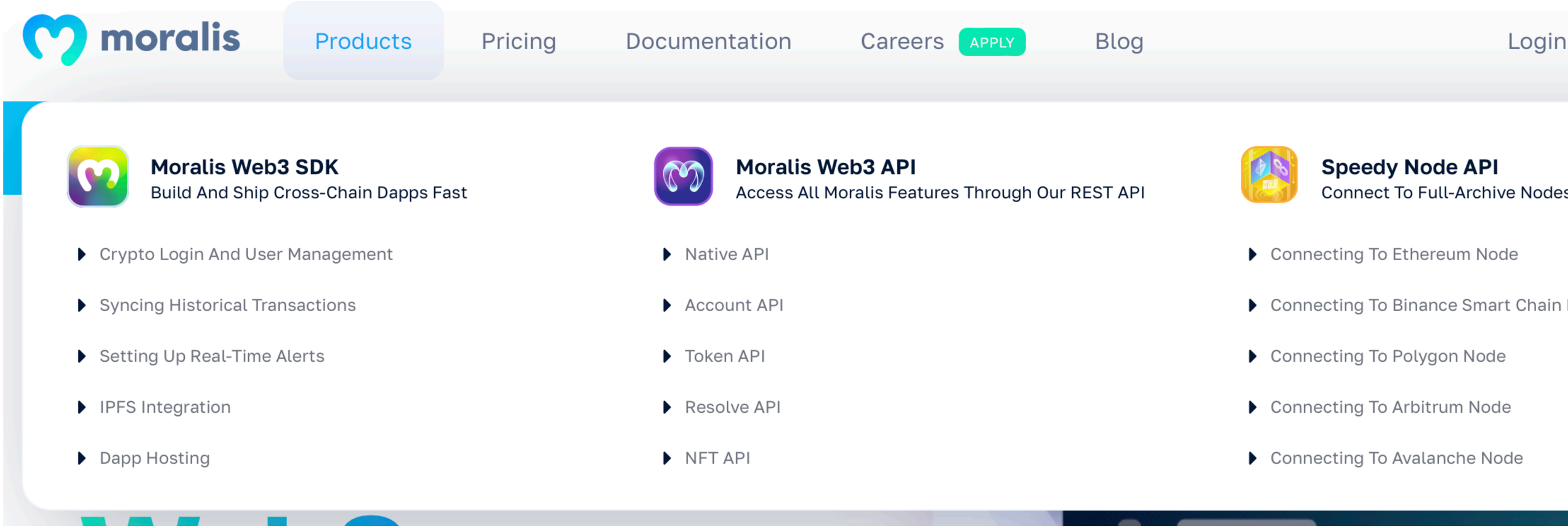
Porque lo importante son los intermediarios



Fuente: https://www.alchemy.com

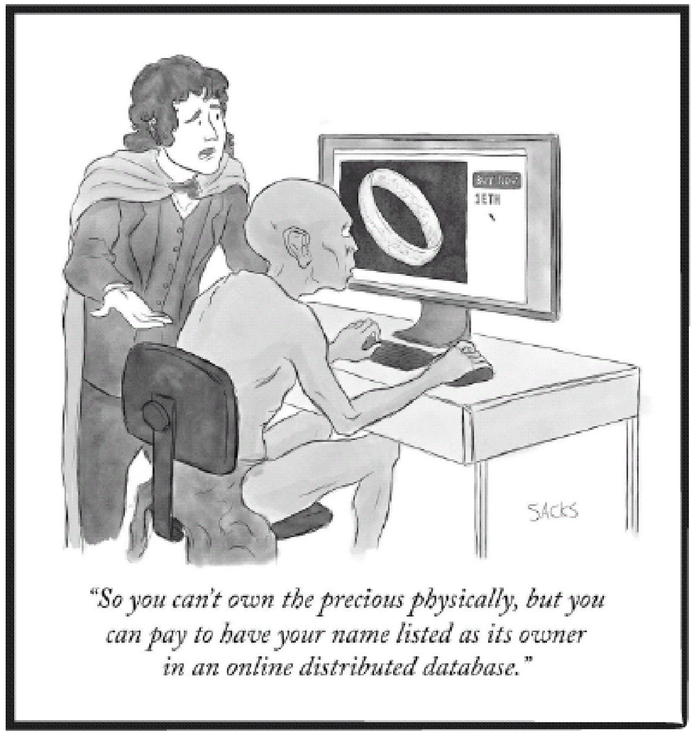
Blockchain as a Service

Porque lo importante son los intermediarios



Web2 + centralización + monetización = Web3

"Yes, the planet got destroyed. But for a beautiful moment in time we created a lot of Bitcoin."



"So you can't own the precious physically, but you can pay to have your name listed as its owner in an online distributed database."

SOURCES (CLOCKWISE FROM TOP-LEFT): TOM TORO VIA STEPHEN DIEHL, ADAM SACKS, JAKE CLARK VIA EXPERTY.IO

Inventemos Web4 porque…
Web3 apesta.

😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱😱

Q&A **&** **Gracias!**