Twitter Thread by Cory Doctorow RIGHT-CLICKING WORDCEL MENTALITY

Cory Doctorow RIGHT-CLICKING WORDCEL MENTALITY
@doctorow

I've just read one of the most lucid, wide-ranging, cross-disciplinary critiques of cryptocurrency and blockchain I've yet to encounter. 1/



It comes from David "DSHR" Rosenthal, a distinguished technologist whose past achievements including helping to develop X11 and the core technologies for Nvidia.

https://t.co/tkAMShno4k 2/

Rosenthal's critique is a transcript of a lecture he gave to Stanford's EE380 class, adapted from a December 2021 talk for an investor conference. 3/

It is a bang-up-to-date synthesis of many of the critical writings on the subject, glued together with Rosenthal's own deep technical expertise. He calls it "Can We Mitigate Cryptocurrencies' Externalities?"

The presence of "externalities" in Rosenthal's title is key. 4/

Rosenthal identifies blockchainism's core ideology as emerging from "the libertarian culture of Silicon Valley and the cypherpunks," and states that "libertarianism's attraction is based on ignoring externalities."

This is an important critique of libertarianism. 5/

The idea that "liberty" is the freedom to do as you like, provided it doesn't harm others is simple enough on its face, but the reality is very few of our actions are free from the potential to harm others. 6/

The freedom to drive, or operate a firearm, or to determine your own vaccination preferences all have impacts on others. 7/

We can (and should) argue about what consideration you owe to your neighbors and what tolerance they owe to you, but all to often, that argument is settled by ignoring it. 8/

Think of the people who talk about masking as a "personal choice." Human beings have an undeniably entwined epidemiological destiny. There are few epidemiological choices that are purely personal - they redound to the people around you. 9/

The existence of a shared destiny and the necessity of a society to manage it runs smack into the idea that messy personal conflicts are best resolved by carving out individual zones of autonomy. 10/

All too often, the libertarian definition of "liberty" is cover for "I don't want to pay taxes to support a society." This is a pretty unpopular position, so libertarians form alliances with naked authoritarians, like the Christian right:

https://t.co/kbmvG5MRbq 11/

That's how you end up with archlibertarians arguing that the world would be "freer" if women weren't allowed to vote:

https://t.co/bIwXOkJfZH

That democracy itself is incompatible with liberty, since it lets workers vote to limi their bosses:

https://t.co/oL2cBCYJMB 12/

The maintenance of libertarian ideology may not require that you ignore externalities, but it sure helps. 13/

When advocates for "liberty" champion the likes of Augusto Pinochet, who tortured and slaughtered his political enemies by the thousands, they are discounting the lethal externalities of Pinochet's economic "freedoms" to zero. 14/

Rosenthal's critique of contemporary blockchainism starts with this idea of discounted externalities - the foundational contradiction that one's "liberty" exists in a state of pristine isolation, and doesn't harm anyone else. 15/

To get to this, he looks at the history of blockchains. He divides blockchain technology into an older, "permissioned" blockchain technology, invented in 1990, and "permissionless" blockchains, which were invented around 2008 with the first Bitcoin white-paper. 16/

A permissioned blockchain require on a central authority that dictates who can write to the chain. Within that stricture, it produces a highly computationally efficient public ledger that can identify malfunctioning or corrupt nodes in the network and route around them. 17/

Permissionless blockchains, like the Bitcoin blockchain, are born decentralized. No one authority gets to decide who can participate in the ledger's creation - at first. This decentralization comes at a high price, though. 18/

Blockchains are vulnerable to "Sybil attacks" where one attacker impersonates a horde of unconnected actors and takes over the system. 19/

To defend against this, permissionless blockchains make Sybil attacks expensive, so that the most you can steal in a Sybil attack is less than it would cost to pull it off. 20/

The inescapable corollary of this is that using the network has to be expensive - the system has to have a giant electricity bill and hence a massive carbon footprint.

This expense, in turn, compensates miners for the money they pour into defeating Sybil attacks. 21/

These miners get paid in cryptocurrency, and for cryptocurrency to have value, it has to have someone who's willing to buy cryptos with "fiat" - dollars or other easily spent money. 22/

The only reason for someone to trade fiat for those cryptos (apart from making ransomware payments) is as an "investment" - that is, because you think the cryptocurrency's price will rise. Thus these blockchains *require* speculation to function. 23/

All of this means that the majority of blockchain activity is just about maintaining the blockchain - not about buying or selling things. There are only about 27,000 "economically meaningful" Bitcoin transactions in a day - and 75% of those are inter-exchange transactions. 24/

All told, only 2.5% of Bitcoin transactions represent someone buying something from someone (fewer than five per minute, globally).

This profound wastefulness is a feature, not a bug. 25/

It's the expense that keeps Sybil attacks at bay, without centralizing authority over the blockchain, as would be the case with the otherwise vastly more efficient permissioned blockchains that have been around for 30 years. 26/

But here's where Rosenthal unveils the other half of his critique: the drive to maximize the efficiency of mining drives miners to consolidate, in order to attain economies of scale. The more valuable a blockchain is, the more centralized it becomes. 27/

Today, 10% of miners control 90% of the mining. The top 0.1% of miners control 50% of mining. Five mining pools control the majority of Bitcoin mining. Last November, only *two* mining pools controlled the majority of Ethereum mining. 28/

This is the worst of all worlds: a highly volatile blockchain that is incredibly wasteful *and* centralized, with control in the hands of largely anonymous parties who are accountable to no one, who can cheat with impunity.

https://t.co/fO5fciIW3u 29/

So far, the focus of Rosenthal's externality critique has been energy consumption and climate harms. But here he comes to his second externality: e-waste. 30/

To maintain their position in the highly concentrated mining sectors, miners have to run their equipment hard and discard it quickly as it burns out. 31/

The average service life of an ASIC used in blockchain mining is a mere 16 months - whereupon it turned into ewaste, retiring its embodied materials and energy. Other blockchain verification systems, like proof of space-and-time, do the same thing to mass storage devices. 32/

Now, it's true that the finance and tech sectors produce a lot of ewaste on their own. But that's because their equipment wears out despite their best efforts to preserve it. 33/

The foundational premise of cryptocurrency mining is that you are in a race with other miners to discard and replace your equipment as rapidly as possible, to eke out every speed advantage. 34/

The blockchainst response to this is to ignore the ewaste problem and hand-wave the emissions issue by claiming that they're fixing it with offsets. Offsets, meanwhile, are a market for lemons. Most carbon offsets are fairy tales:

https://t.co/xbJRf73SZy 35/

And, as Rosenthal points out, even if your cryptos are being mined with renewables, that is only carbon neutral if you assume "that doing so doesn't compete with more socially valuable uses for renewables, or indeed for power in general." 36/

Blockchainists are aware of the problems with proof of work, and many are calling for a transition to proof of stake, a notionally less climate-intensive way of running a permissionless blockchain. 37/

Rosenthal's critique of proof of stake begins by observing that it drives even more centralization than proof of work. 38/

A proof of stake network allows the people who have the most to tax the transactions of those with less, cementing their dominance and increasing centralization. 39/

So both permissioned and permissionless blockchains end up centralized, but permissionless blockchains - the type beloved of blockchainists - are centralized into unaccountable and often anonymous hands. 40/

So while a permissioned blockchain that is run by a benevolent (or at least accountable) authority can reverse frauds, permissionless blockchains struggle to do this. 41/

This immutability is part of the reason that blockchains and fraud go together like peanut butter and chocolate. Thefts on working permissionless blockchains can't be readily reversed, making them permanent. 42/

Meanwhile, the entities who end up at the top of the centralization pile in these networks can commit thefts by rewriting the "immutable" ledgers. 43/

It's not a purely hypothetical problem. The Steem proof of stake network was compromised by Justin Sun in 2021, who took advantage of the highly centralized staking sector to hijack the Steem blockchain. 44/

The immutability problem is worse in programmable cryptos like Ethereum. The "smart contracts" that operate on these chains are effectively bug bounties whose maximum payout is everything in the wallets connected to them. 45/

The attack surface of programmable money which is connected to social media, Discord servers, standalone wallets, etc, is virtually unbounded. 46/

This is another important point raised by Rosenthal: not only are permissionless blockchains highly concentrated, they're also ineluctably bound up with Web 2.0 technologies. 47/

The fact that Binance conducts two thirds of crypto derivative transactions and half of all spot technologies using browsers and other 2.0 stuff multiplies all the blockchain vulns by all the non-blockchain vulns. 48/

Here Rosenthal cites Adam Levitin's recent, excellent analysis of the legal status of crypto exchange users in bankruptcy proceedings (tldr: if your exchange goes bust, you'll probably get nothing or nearly nothing):

https://t.co/jdtbWjOe3C 49/

Rosenthal's boils this all down to four points:

I. Permissioned blockchains can stop Sybil attacks without cryptocurrency and have no significant externalities; 50/

II. Permissionless blockchains *require* a cryptocurrency to stop Sybil attacks, and this produce major externalities;

III. To be successful, permissionless blockchains require proof-of-work or some other deliberately wasteful system, making externalities inevitable; 51/

IV. Likewise inevitable is that any security system based on wasting resources will create the centralization that permissionless blockchains claim to eliminate. 52/

Rosenthal concludes his talk by affirming that he values decentralization and it is that value that causes him to reject blockchainism. 53/

He reminds us that the billions pouring into the Web3 bubble are bets on attaining scale and dominance - the only reason to pump billions into a blockchain technology is if you think that you can corner a market and make it back. 54/

In other words, Web3 investors see high barriers to entry as a feature, not a bug, and they're committed to centralization. 55/

Image:
U.S. Fish and Wildlife Service Headquarters (modified)
https://t.co/bq5JJPcDcp

CC BY 2.0:
https://t.co/B930sKCLnf 56/

ETA - If you'd like an unrolled version of this thread to read or share, here's a link to it on https://t.co/iSBh8s9m7q, my surveillance-free, ad-free, tracker-free blog:

https://t.co/5rhyfeEW7L