Statement of Prof. Ari Juels

Faculty Member at Cornell Tech
New York, NY

Submitted to the U.S. House Energy and Commerce Committee,
Subcommittee on Oversight and Investigations,
for the hearing

Cleaning Up Cryptocurrency: The Energy Impacts of Blockchains

January 20, 2022

Testimony

Chair DeGette, Ranking Member Griffith, Chairman Pallone, and Ranking Member Rodgers, thank you for inviting me to speak to you today. My name is Ari Juels. I'm a faculty member at Cornell Tech and Cornell University. My main area of research is blockchain technologies.

If my testimony achieves nothing else today, I would like to drive home one key point. *Bitcoin does not equal blockchain.* The tremendous promise of blockchain technology does not require Bitcoin or its energy-intensive component called *proof of work*. In fact, some of the most exciting developments in the blockchain industry today are happening outside the Bitcoin ecosystem.

There's a lot of mystification around blockchain technology. But the basic goal is actually fairly simple. A blockchain aims to realize a kind of *digital bulletin board*, sometimes called a *ledger*. This bulletin board has some special properties. It's *globally readable*, meaning that everyone in the world sees all posted messages and sees them in the same order. It's also *immutable*. A message, once posted, can never be altered or removed.

Such a digital bulletin board as realized by a blockchain is conceptually simple but powerful. For example, it can support a global payment system. Suppose that the messages posted to the bulletin board specify authentic money transfers. A message might say, "I, Alice, send one dollar to Bob." Because the bulletin board is globally readable, any person in the world can determine the monetary balance of all users of the system. You just need to tally up all of the money transfers in posted messages. Substitute Bitcoin for dollars and random numbers for names, and what I've presented is a grossly simplified but essentially accurate picture of how cryptocurrencies such as Bitcoin work.

You could realize this digital bulletin board using an ordinary web server, the kind you interact with every day on the internet. But if that server crashes or is hacked, the bulletin board will fail. The brilliant insight of Bitcoin's inventor was a way to avoid such problems using a blockchain maintained by an open community. To ensure fair participation, and that no one individual can easily take over the system, Bitcoin relies on what's called *proof of work*. To help maintain the Bitcoin blockchain and earn Bitcoin through a process called *mining*, you need to contribute a large amount of computation to the system. You do this by solving hard mathematical puzzles. Unfortunately, Bitcoin mining consumes a massive amount of electricity. Credible estimates place this consumption today at roughly half a percent of the world's total electricity supply—more, for instance, than the entire nation of Argentina.

The term "proof of work," I should say, was coined in a scientific paper I co-authored back in 1999. A decade before the advent of Bitcoin, that paper already recognized the inherent waste in proof of work. The paper was therefore about how to recycle proof-of-work computation.

Happily the blockchain community has devised new ways to realize blockchains without proof of work. The leading alternative, which consumes far less electricity, is called *proof of stake*. The

number-two cryptocurrency, Ethereum, plans to adopt proof of stake. Nearly all new blockchain systems already use it today to secure hundreds of billions of dollars in value. These systems are faster than Bitcoin and support what are called *smart contracts*, small programs that run on blockchains. Smart contracts are powering some of today's most exciting blockchain applications, including what's called decentralized finance or DeFi and non-fungible tokens or NFTs. Bitcoin doesn't readily support DeFi or NFTs today. Again, Bitcoin does not equal blockchain.

Proof of work is heavily battle-tested and has valuable theoretical security properties, but there are many misguided claims made about it. For instance, some claim it is critical to achieving *decentralization*, meaning broad participation. But Bitcoin and in fact many blockchain systems are in some key ways notably centralized; this is a challenge the whole industry is working on. For example, in the case of Bitcoin, just four entities, called *mining pools*, today control a majority of the mining power and thus technically can control the whole system.

In summary, the Bitcoin community deserves our deep gratitude for introducing blockchains to the world. But we have far more energy efficient alternatives than proof of work. For the sake of the environment and our energy infrastructure in the United States, I believe that we need to embrace these newer options.

Supplementary materials

- **Bitcoin energy consumption:** While measuring Bitcoin energy consumption requires some guesswork, roughly accurate estimates are possible. One good such estimate is provided by the Cambridge Bitcoin Electricity Consumption Index.[1]
- **Bitcoin centralization / decentralization:** As of January 17, 2022, the mining pools Foundry USA, Antpool, F2Pool, and Poolin together controlled over 50% of the total mining power, enough in principle to control the Bitcoin network.[2] (Such centralization of control affects not just Bitcoin. The situation is similar in other blockchain systems as well.)
  Note that it is true that many thousands of mining devices (known as *mining rigs*) participate in Bitcoin mining through these pools. It is also true that some of these devices may be owned by entities other than the operator of the mining pool in which they participate. But a multiplicity of devices does not equate with decentralization. At issue is *who controls* the mining devices. In a mining pool, the pool operator determines *what blocks the mining devices mine*, and in that sense controls them.
  Apart from mining-pool centralization, Bitcoin and other blockchain systems are notably centralized in other key respects as well.[3] [4] The blockchain industry as a whole is working to achieve stronger decentralization of blockchain systems.
- **Proof-of-work (PoW) vs. proof-of-stake (PoS) security:** There has been considerable debate as to whether PoS is or can be as secure as PoW. It is difficult to compare the security of PoW and PoS directly, however. The two systems are incomparable, in the sense that their security relies on different sets of assumptions. In some sense, however, this debate is now moot: *PoS systems are currently securing hundreds of billions of dollars of value in blockchain environments as adversarial as Bitcoin's*. In other words, there is a financial incentive for hackers to mount successful attacks against proof-of-stake blockchains, yet major attacks have not materialized.
  Indeed, it is notable that there have been no foundational attacks against important PoS systems in the wild, whereas there have been multiple successful attacks against medium-size PoW systems.[5] Bitcoin has achieved the remarkable feat of running continuously, without serious disruption, for more than a decade, but it relies critically today on the massive resources in its network to achieve its strong security.

---

[1] Referenced at https://ccaf.io/cbeci/index/comparisons.
[2] See, e.g., https://btc.com/stats/pool.
[3] Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE security & privacy*, *12*(3), 54-60. Available online here.
[4] Makarov, I., & Schoar, A. (2021). *Blockchain Analysis of the Bitcoin Market* (No. w29396). National Bureau of Economic Research. Available online here.
[5] Voell, Z. Ethereum Classic Hit by Third 51% Attack in a Month. *CoinDesk*. Aug. 29, 2020. Available online here.

PoW does have some appealing security properties. Prime among these is that PoW security is *physically anchored*, in the sense that generating blocks in a PoW blockchain requires investment of physical resources (equipment and electricity) and thus the validity of a PoW blockchain depends on external or "objective" resources. PoS relies on an internal resource (cryptocurrency). It is therefore easier in theory to forge a PoS blockchain than a PoW blockchain. In practice, however, there is no compelling evidence that reliance on external vs. internal resources is an important contributor to the global security of a blockchain. For instance, the various forms of centralization in blockchains noted above can erode the "objectivity" provided by its PoW mining. As a simple example, a small number of entities write software employed by a large fraction of users, e.g., wallet software. There have been instances of user wallets violating basic properties of, e.g., the Bitcoin network,[6] and malicious wallets can in general deceive users in any number of ways.

Claims are sometimes made that PoW is preferable to PoS because unlike the case in PoW systems, in PoS systems, rewards are proportional to investment of cryptocurrency. Thus, it is claimed, in PoS systems, the rich get richer. While PoS systems can cause the rich to grow richer, research suggests that this is not a fundamental property of PoS, but a question of how it is deployed.[7] Moreover, Bitcoin and many other blockchain systems already have a highly skewed distribution of wealth.[8] [9] In PoW systems, the centralization of mining power and the ability of large entities to benefit from economies of scale in mining operations is one factor in such inequality.

- **Mining-device energy efficiency:** Proof-of-work mining proponents sometimes point out that mining equipment is growing more energy efficient. This is true in terms of computational power per watt for *individual mining devices* (also known as *mining rigs*). But because *relative mining power* determines profits and not *absolute mining power*, improvements in the efficiency of individual devices does not translate into improvement of the energy efficiency of the *network as a whole*. In fact, Bitcoin's global electricity consumption has grown steadily over time—particularly over the past year.[10] The same is true of other proof-of-work blockchains.
- **Use of renewables for proof-of-work mining:** If proof-of-work mining is unavoidable, then leveraging such mining to facilitate the development of renewable-energy infrastructure or to consume excess electricity is certainly more desirable than use of

---

[6] Gervais, A., Karame, G. O., Capkun, V., & Capkun, S. (2014). Is Bitcoin a decentralized currency? *IEEE security & privacy*, *12*(3), 54-60. Section 3.1. Available online here.

[7] Fanti, G., Kogan, L., Oh, S., Ruan, K., Viswanath, P., & Wang, G. (2019, February). Compounding of wealth in proof-of-stake cryptocurrencies. In *International conference on financial cryptography and data security* (pp. 42-61). Springer. Available online here.

[8] Vigna, P. (2021). Bitcoin's 'One Percent' Controls Lion's Share of the Cryptocurrency's Wealth. *The Wall Street Journal*. December 21, 2021. Available online here.

[9] Schultze-Kraft, R. (2019). Assessing the Distribution of ERC20 Tokens on the Ethereum Network: On-Chain Metrics Show Highly Uneven Token Distribution Across ERC20s. Available online here.

[10] See, e.g., https://ccaf.io/cbeci/index.

less sustainable alternatives. There are two important considerations, however, in the use of renewable or excess energy for proof-of-work mining:

- **Opportunity cost**: Rather than being used for proof-of-work mining, renewable or excess energy might be used for other forms of high-performance computing (e.g., drug discovery) or for energy-intensive industrial processes (e.g., smelting bauxite) or might be stored for later use given suitable energy-storage technology (e.g., batteries). Even if such alternatives are not immediately viable or competitive, by favoring proof-of-work mining, we risk impeding their development.
- **Competing cheap energy:** Even if a large fraction of proof-of-work mining makes use of renewable energy, it is important to take into account any sizeable fraction that *does not*. Miners have a financial incentive to chase the cheapest forms of energy across the globe, irrespective of the harmful effects. Kazakhstan offers a recent example. In the wake of China's recent ban on cryptocurrency mining, a number of Bitcoin miners relocated to Kazakhstan, which quickly became the world's second-biggest crypto-mining country (after the U.S.). Kazakhstan generates some of the dirtiest energy in the world.[11] [12] Additionally, Bitcoin mining overloaded the electric grid and contributed to blackouts, a component in the recent civil unrest in the country.[13]

- **Bitcoin functionality:** The Bitcoin network typically handles fewer than five transactions per second, and has an estimated peak capacity of seven transactions per second.[14] In contrast, the Visa payment processing network handles roughly 1,700 transactions per second,[15] with a claimed peak load of some 24,000 transactions per second.[16] (One reason that Ethereum is migrating to proof-of-stake—and embracing other changes—is that, like Bitcoin, it suffers from slow transaction rates and cannot meet user demand cost-effectively.)

  The cost per Bitcoin transaction varies over time. It is currently, as of January 17, 2022, roughly $1.50 per transaction. It is volatile, however, and has at times reached tens of dollars per transaction.[17]

  Bitcoin is not in general functional today as a broad means of payment, i.e., medium of exchange. In that sense, it does not fulfill one of the basic roles of money or currency, as

---

[11] Tully, S. (2022). Kazakhstan internet shutdown sheds light on a big Bitcoin mining mystery. *Fortune*. January 5, 2022. Available online here.

[12] Kazakhstan. International Energy Agency Country profile. Referenced online on Jan. 17, 2022. Available online here.

[13] Muir, M. (2021). Crypto miners in Kazakhstan face bitter winter of power cuts: Illegal miners and mass relocations after ban on crypto mining in China have overloaded energy grid. *Financial Times*. Nov. 25, 2021. Available online here (behind paywall).

[14] Croman, K., Decker, C., Eyal, I., Gencer, A. E., Juels, A., Kosba, A., ... & Wattenhofer, R. (2016, February). On scaling decentralized blockchains. In *International conference on financial cryptography and data security* (pp. 106-125). Springer, Berlin, Heidelberg. (Note: The peak transaction rate is probably higher at this point, but there are no good up-to-date studies.) Available online

[15] Based on the claim that the network processes 150 million transactions a day. See https://usa.visa.com/run-your-business/small-business-tools/retail.html.

[16] Ibid.

[17] See, e.g., https://www.blockchain.com/charts/fees-usd-per-transaction.

such instruments are conventionally defined.[18] Since 2015, the Bitcoin community has been working to improve Bitcoin transaction rates by means of a supplementary system called the Lightning Network.[19] [20] There have been helpful recent technical additions to Bitcoin in support of the Lightning Network,[21] but also serious concerns, for instance around privacy.[22] [23] In brief, the Lightning Network is promising, but is currently at an early stage of development.

Disclosures:

- I am a Co-Director of the Initiative for Cryptocurrencies and Contracts (IC3). Website: www.initc3.org. IC3 receives funding from industry partners listed here: https://www.initc3.org/partners.html.
- I am Chief Scientist at Chainlink Labs. Website: https://chainlinklabs.com/.
- I serve as a technical advisor to Soluna Computing, Inc. Website: https://www.solunacomputing.com.
- I have personal holdings of cryptocurrencies and tokens.

[18] Federal Reserve Bank of St. Louis. Functions of Money - The Economic Lowdown Podcast Series. Online resource, accessed January 17, 2020. Available online here.

[19] Poon, J., & Dryja, T. (2015). The Bitcoin Lightning Network*:* Scalable off-chain instant payments. Version from 2016 available online here.

[20] See https://lightning.network/.

[21] Hertig, A. 5 Ways Bitcoin's Lightning Network Advanced in 2021. *CoinDesk*. December 28, 2021. Available online here.

[22] Kappos, G., Yousaf, H., Piotrowska, A., Kanjalkar, S., Delgado-Segura, S., Miller, A., & Meiklejohn, S. (2020). An empirical analysis of privacy in the Lightning Network. *arXiv preprint arXiv:2003.12470*. Available online here.

[23] Lin, J. H., Primicerio, K., Squartini, T., Decker, C., & Tessone, C. J. (2020). Lightning Network: a second path towards centralisation of the Bitcoin economy. *New Journal of Physics*, *22*(8), 083022. Available online here.