United States Senate, Committee on Energy and Natural Resources
Hearing on Energy Efficiency of Blockchain and Similar Technologies

Responses to Questions for the Record

Arvind Narayanan
Associate Professor of Computer Science, Princeton University

Chairman Murkowski, Senator Manchin, and members of the committee, thank you for the opportunity to respond to questions for the record. I would also like to take this opportunity to correct an error in an estimate that I provided in my written testimony. I have done so in an Appendix to this document. I sincerely regret my error.

Questions from Chairman Lisa Murkowski

Question 1: You have testified that a blockchain "is a sequence of records that is collectively maintained by a set of stakeholders and is designed to support the addition of records while resisting modification or deletion of existing records."

· At what point does the length of a blockchain provide diminishing returns for security and verification purposes?

· Would setting a cut-off point for the number of blocks on a chain (i.e., dropping blocks on the back end as new blocks are created) allow for any energy efficiencies – and less energy needed for mining purposes – for proof of work or data storage requirements?

Response. There are broadly two sources of inefficiency in blockchains. The first is the need for participants to track transactions, verify their validity, and perform other maintenance activities. It is indeed true that as a blockchain grows, keeping track of all transactions leads to increasing data storage requirements. Most blockchain designs do include the ability for participants to drop or "prune" old records to decrease their storage costs. This is an area of ongoing research and innovation.

However, pruning does not address the second source of inefficiency, namely the energy needed for mining purposes. The large computational requirements of mining arise not because of the need to track or verify transactions. Rather, it involves a separate type of calculation that performs no useful function except to deter adversaries from attempting to disrupt the blockchain's operation. Thus, it is precisely the computational inefficiency of mining that allows it to fulfill the function of securing the blockchain. The difficulty of the mining calculations does not vary based on the length of the blockchain.

Fortunately, mining is used only in public blockchains that support cryptocurrencies. The envisioned applications of blockchain technology in the energy industry involve private blockchains which have no need for mining. This is because a majority of stakeholders are assumed to be trustworthy and there is no risk of an unknown adversary attempting to subvert the system.

<u>Question 2</u>: Blockchain is often promoted as a means to achieve anonymity in market transactions. But much of the trading in energy markets has no need for anonymity. For example, two state-owned utilities may not need or want to keep their transactions anonymous.

· In a market where anonymity is less important, does that reduce the value of blockchain techniques?

<u>Response.</u> Indeed, there is no need for anonymity in energy trading and other applications in the energy industry. While many blockchains, especially public blockchains, enable a degree of anonymity, that is not an inherent property of blockchains. Blockchain-based energy trading can be combined with strong identity assurance of market participants.

Questions from Senator Joe Manchin III

<u>Question 1</u>: In effort to reduce overhead costs, developers look to areas that offer cheap electricity and cool climates. However, some communities across the country are dealing with the impacts of increased electricity prices due to the demands of the data centers. According to your written testimony, "the increasing energy efficiency of mining hardware has essentially no impact on energy consumption." Can you please discuss the efficiency of these deployed mining machines, and what local leaders should be aware of for those communities where they are being considered by cryptocurrency developers?

<u>Response.</u> Inefficiency is deliberately designed into mining-based blockchains. When more efficient mining hardware is developed, mining becomes more profitable, which incentivizes more computing power to be dedicated to mining. Blockchain protocols are designed to react to such an increase in mining capacity by proportionally increasing the computational difficulty of mining. In this way, the effect of the increasing efficiency of mining hardware gets nullified by the increasing difficulty of mining, and thus there will be little or no net impact on mining energy consumption.

Cryptocurrency miners are different from many other types of industrial electricity consumers because their revenues are dependent on cryptocurrency exchange rates, which tend to be highly volatile. Demand for mining tends to increase or decrease relatively quickly in response to cryptocurrency exchange rate fluctuations. This unpredictability might create difficulty for communities. One potential way for local leaders to manage this unpredictability is to establish (possibly informal) communication channels with the cryptocurrency mining community, which would give leaders advance knowledge of trends in mining demand.

<u>Question 2:</u> What role, if any, can FERC have to provide oversight of blockchain technologies in the energy industry?

<u>Response.</u> Blockchain technology is relatively new and there are uncertainties in a number of areas, such as the legal status of transactional records stored on blockchains. Another concern is the “endpoint” cybersecurity risk, that is, the risk of compromise of the devices that store participants’ private keys and protect their digital assets stored on the blockchain. There is a need for regulatory oversight in promulgating requirements for record-keeping systems to be considered authoritative, as well as in setting cybersecurity standards for the computing systems used in the grid.

Appendix: correction of an error in written testimony

In my written testimony, I stated:

> An accepted method for deriving an estimate of the energy consumption of mining is to assume that all miners use the most energy efficient mining device available on the market.[1] Commercial devices are accompanied by published specifications listing the number of hashes that can be computed per second using the device, as well as the power consumption of the device in watts. It is then straightforward to calculate how much power is required to compute 50 billion billion hashes per second using the most energy efficient devices available. I performed such a calculation and obtained an estimate of around 5 gigawatts for Bitcoin mining alone today.[2] This is slightly under 1% of world electricity consumption, or slightly more than the electricity consumption of the state of Ohio or that of the state of New York. Other public blockchains also consume a substantial, albeit much lower, amount of energy.

The 5 gigawatt estimate of Bitcoin mining energy consumption, including the footnotes, remains correct to the best of my knowledge. However, the comparisons to the electricity generation / consumption of the world and U.S. states are incorrect. An electricity consumption of 5 gigawatts translates to 44 terawatt hours per year. According to the International Energy Agency, world electricity generation in 2017 was 25,570 terawatt hours,[3] which puts Bitcoin mining energy consumption at around 0.2% of this figure, rather than "slightly under 1%" as I stated previously. I sincerely regret the error.

---

[1] *See* Alex de Vries, *Bitcoin's Growing Energy Problem*, 2 Joule 801-805 (2018), https://www.cell.com/joule/fulltext/S2542-4351(18)30177-6; Arvind Narayanan et al., *Bitcoin and cryptocurrency technologies: a comprehensive introduction*, Princeton University Press (2016), http://bitcoinbook.cs.princeton.edu/.

[2] The most energy efficient mining device known to be in widespread use is the Bitmain Antminer S9, which achieves an efficiency of 10 billion hash computations per Joule of energy, resulting in an estimate of 5 gigawatts for Bitcoin mining. Recent announcements of new devices have claimed higher mining efficiencies; if these are in widespread use, the true power consumption might be slightly lower than 5 gigawatts. On the other hand, some devices in use may be much less efficient, which would mean that the true power consumption might be higher. Further, accounting for the energy consumption of cooling of mining data centers would also increase the estimate.

[3] International Energy Agency, Global Energy & CO2 Status Report 2017 (March 2018).