Written Testimony of Arvind Narayanan
Associate Professor of Computer Science, Princeton University

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

August 21, 2018

Chairman Murkowski, Ranking Member Cantwell, and members of the Committee, I thank you for the opportunity to testify about blockchain technology and its implications for energy efficiency and cybersecurity.

My name is Arvind Narayanan, and I am an associate professor at Princeton University. I am a computer scientist, and my main research areas are information privacy and cybersecurity. I have been researching blockchain technology since 2013 and have authored numerous peer-reviewed publications in this field. I have taught courses on cryptocurrencies and blockchains since 2014. I am a lead author of a textbook on the topic that has been used in over a hundred courses around the country and worldwide.

In this testimony, I will address three topics. First, I will provide an overview of blockchain technology. Second, I will describe the energy consumption associated with certain blockchains. I will explain why these blockchains consume a large amount of energy for their upkeep, and offer an opinion on how we can expect this consumption to evolve. Third, I will discuss the potential applications of blockchain technology in the energy industry. I will focus on the potential to improve cybersecurity and efficiency, while also highlighting the limits of blockchain technology and alternatives that might achieve the same goals.

1. Overview of blockchain technology

The term blockchain is used to describe a loosely related collection of technologies. What they have in common 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. This is achieved by a technological mechanism that protects the integrity of the data even if any minority of participants attempt to undermine it.

Hundreds of blockchains exist today. The vast majority follow one of two basic designs. In public blockchains, also called permissionless blockchains, anyone may become a maintainer of the records. In the most prominent public blockchains today, maintaining the records involves a computationally intensive process called mining.[1] It requires mathematical calculations by a large number of computers working in parallel. This is by deliberate design: the aim is to ensure that any adversary aiming to disrupt the integrity of the system must control and operate, at

[1] I discuss mining-free public blockchains in the next section.

least momentarily, as much computing power as the rest of the miners. In other words, it is precisely the computational difficulty of mining that makes public blockchains hard for adversaries to attack.

Miners are compensated for their effort in maintaining the integrity of the blockchain. To enable this, each public blockchain is paired with a virtual currency, also known as a cryptocurrency. Addition of records to the blockchain triggers an algorithm to issue new units of the cryptocurrency, which are paid out as revenue to the miners. The blockchain in turn supports the operation of the cryptocurrency by serving as an authoritative record of cryptocurrency transfers. Since the blockchain is resilient to modification, participants trust the veracity of this record and use it to execute trades and determine currency balances. In other words, the blockchain is the technology platform necessary for the operation of the cryptocurrency, and the cryptocurrency incentivizes miners to maintain the blockchain. Neither would exist in a useful form without the other.

In contrast to public blockchains, private blockchains (also called permissioned blockchains or consortium blockchains) work very differently. Maintenance of the records is limited to a pre-specified list of entities, such as a consortium of banks or a consortium of utilities. Since a majority of stakeholders are assumed to be trustworthy and there is no risk of an unknown adversary attempting to subvert the system, mining is not necessary. Nor is a cryptocurrency needed for the functioning of private blockchains, although many such blockchains do support cryptocurrencies or other digital tokens. Finally, private blockchains tend to have a high capacity or throughput, that is, they support a high rate of addition of new records, whereas public blockchains are inherently limited in this respect.

	Public blockchains	**Private blockchains**
Who maintains the blockchain	Anyone may participate anonymously	Limited, known set of participants
Relationship to cryptocurrency	Must be paired with a cryptocurrency	Cryptocurrency not necessary, but sometimes supported
Energy efficiency	Most prevalent design requires energy-intensive mining	Does not involve mining
Capacity (records added per second)	Inherently limited	High capacity achievable

Table: comparison of public and private blockchains

2. Implications of blockchains for energy efficiency

On today's most prominent public blockchains, mining involves the computation of a large number of mathematical calculations, called hashes, in parallel. For example, as of this writing, miners of Bitcoin, the original blockchain-based cryptocurrency, collectively compute about 50 billion billion hashes, or 50 billion gigahashes, every second.[2] Most mining is carried out in large-scale commercial operations using purpose-built computing devices specialized to the task of repeatedly computing these hashes — and nothing else. These devices are housed in warehouses dedicated to mining, usually called data centers. Substantial energy is required to operate the computing devices as well as to cool them to keep them within their operating temperature limits.

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.[3] 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.[4] 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.

To understand how this number might change over time, economists use equilibrium models of mining.[5] Miners produce a virtual commodity in a competitive market. Miners will enter this market if it is profitable to mine and drop out if it is not, driving the market toward zero profit. Further, mining is a zero-sum game: the total revenue that can be earned per time unit by mining a specific cryptocurrency is fixed. In the case of Bitcoin, it is roughly 12.5 bitcoins every 10 minutes.[6] In mid-August 2018, the exchange rate is roughly USD 6,500 per bitcoin, making

[2] An estimate of the current rate of hash computation is available at: https://www.blockchain.com/en/charts/hash-rate

[3] *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/.

[4] 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.

[5] de Vries, *supra* note 3.

[6] To be more precise, Bitcoin miners earn revenue from two sources: from newly minted units of cryptocurrency, and from transaction fees that cryptocurrency users pay to miners. The rate of minting of Bitcoin halves every four years. It is next scheduled to halve in mid-2020 from 12.5 bitcoins to 6.25 bitcoins every 10 minutes. Transaction fees are determined by a market mechanism; they currently

the mining revenue worth roughly USD 80,000 per 10-minute period. However, the exchange rate tends to fluctuate substantially. Against these revenues, miners have costs including electricity, mining hardware, and other costs of operating mining data centers. Electricity costs are a substantial fraction of overall costs — a fraction that is relatively stable over time. For example, if we use a ballpark figure of 50% for this fraction, the equilibrium model suggests that Bitcoin miners currently collectively expend roughly USD 6 million per day worth of electricity.

To summarize, the main variable in the equation that governs the energy consumption of cryptocurrency mining at equilibrium is the exchange rate between the cryptocurrency and dollars. Other factors such the amount of cryptocurrency available to mine per unit time have minor impacts on energy consumption, but they cannot explain the orders-of-magnitude increase in mining energy consumption that we have witnessed over the last few years. Roughly speaking, if the price of a cryptocurrency goes up, more energy will be used in mining it; if it goes down, less energy will be used. Little else matters. In particular, the increasing energy efficiency of mining hardware has essentially no impact on energy consumption.

Several attempts have been made to design public blockchains that don't require mining. The security of these designs is not as well understood theoretically or as well tested practically as that of mining-based blockchains; it is an active area of research and development. The developers of Ethereum, the second largest blockchain by market capitalization, have announced a goal of switching Ethereum to a mining-free model. However, the developers and the community behind Bitcoin have strongly resisted major changes to its design. In my opinion, this is likely to continue. Since Bitcoin is by far the largest consumer of cryptocurrency mining energy, this makes it unlikely that the maturation of mining-free public blockchain technology will have a short-to-medium-term impact on overall energy consumption in the blockchain sector. However, the long-term impact is harder to predict.

The above analysis pertains to the cumulative, worldwide energy consumption of public blockchains. A question remains as to where miners will choose to locate their operations. Cost considerations tend to dominate the geographic distribution of mining activity: low electricity prices and cooler climates (which leads to lower data center cooling costs) are attractive for mining. Policy incentives and disincentives such as taxes can also play a significant role.

3. Implications of blockchain technology for the energy industry

Just as blockchains can be used to record transfers of cryptocurrencies, they can be used to record transfers of other assets that can be represented digitally, such as commodities and derivatives. Since a blockchain can record both transfers of assets and payments for those assets, it can serve as a platform for a digital market. Indeed, a blockchain-based market for Internet

remain a small component of mining revenue, at a fraction of a bitcoin per 10-minute interval, but it is believed that as the minting reward dwindles, transaction fees will gradually increase. Most other mining-based cryptocurrencies follow this overall reward structure, but with differing specifics. Regardless of these nuances, at a high level, the amount of mining revenue available to be earned is not directly affected by the number of miners who compete to earn it, or the computational power they bring to bear.

domain names has existed since 2011, and numerous other blockchain-based markets are in various stages of development and deployment.[7]

Proponents of such markets view it as a benefit that unlike traditional digital markets, no single entity acts as a gatekeeper with the power to determine who is allowed to trade and who isn't. Another purported benefit is that transaction data would be accessible by all market participants, enabling more efficient trading. Finally, blockchain-based markets may improve efficiency and decrease settlement time compared to one where trades are settled using paper records or otherwise require human intervention. On the other hand, they tend to be less efficient compared to centralized digital markets.

In practice, blockchain applications have often fallen short of claimed benefits. One recurring pattern is that the development new blockchains is difficult to accomplish without a degree of central coordination, and the technology developers inevitably possess a significant ability to control the resulting platform. In at least one instance, a blockchain-based platform for voting was controlled by a single company, arguably negating the putative benefits.[8]

In the energy sector, several initiatives exist for utilizing blockchain technology in the context of both wholesale and consumer markets.[9] Such blockchains are typically run by consortia of utilities or energy companies, and are thus private blockchains. Some initiatives enable firms to trade bulk quantities of power, gas, other commodities, and options on those commodities. A blockchain-based market might be more attractive than a centralized trading platform if market participants are averse to a single company controlling the platform. Other initiatives enable customers to directly trade electricity with each other in a "peer to peer" fashion, for example, by buying and selling excess rooftop solar power. However, peer-to-peer trading still requires the cooperation of utilities who ultimately control the physical flow of electricity.

Another envisioned application combines energy trading with automated control of energy consumption. This requires granular electricity prices based on time and location. If such a market existed, a refrigerator, for example, might contain a software controller that monitors energy prices, ambient temperature, and other factors to make decisions about power consumption at any given moment. Such automated controllers are often termed smart contracts. In my opinion, smart contracts for controlling energy consumption and generation can be adopted largely independently of blockchain technology.

To summarize, blockchains have the potential to underpin various types of energy markets, both existing and new. Many of these applications are currently speculative and blockchain technology is only one route to realizing them, with potential benefits as well as drawbacks.

[7] The market for Internet domain names is called Namecoin (https://namecoin.org/). Other markets include Augur (https://www.augur.net/), a prediction market, and proposals in the finance industry. *See* Nasdaq, *Building on the Blockchain Nasdaq's Vision of Innovation* (2016), https://bit.ly/2BuXQnU.

[8] *See* David Gerard, *West Virginia and the Voatz "blockchain" voting system — scaling and security concerns* (2018), https://bit.ly/2BnX0JR

[9] *See* David Livingston et al., *Applying Blockchain Technology to Electric Power Systems*, Council on Foreign Relations Report (2018), https://bit.ly/2vWfmfN

Blockchains and the cybersecurity of the grid

As the nation's electric grid and energy systems become more digital, cybersecurity risks arise: adversaries who exploit digital vulnerabilities to penetrate networks might be able to interfere with the grid's operation even without physical access to critical infrastructure.[10] Like any digital system, securing the computing systems that supply our energy comes down to the protection of their confidentiality, integrity, and availability.

Confidentiality means keeping sensitive information from falling into the hands of unauthorized parties. Integrity means preventing unauthorized modifications to data and authenticating its origin. Availability means ensuring the smooth operation of computing systems and the accessibility of information to authorized parties when needed.

Today's information security best practices incorporate cryptography as a key vehicle for achieving these goals. Encryption, when properly implemented, aids greatly in ensuring confidentiality. Similarly, digital signatures and message authentication codes are vital tools for achieving data integrity. For example, an attacker who infiltrates a part of the network might be able to spoof a signal from a sensor or an intelligent electronic device, resulting in the issuance of rogue control commands, such as tripping circuit breakers. A design that aims to mitigate such attacks would require control commands to be accompanied by message authentication codes. The receiving device or system would verify the code before executing the command. If the keys were stored securely, the attacker would not be able to spoof the code without a compromise of physical security.

While these techniques have similarities to the manner in which blockchains ensure data integrity, blockchain technology is not necessary for achieving most of the cybersecurity benefits of cryptography in energy systems. That said, blockchain technology has the potential to provide additional cybersecurity benefits.

First, blockchains offer an alternative route to data integrity that provides an authoritative record of the date and time of transactions and other messages. Second, blockchains can enable rapid detection of (and recovery from) breaches. If all actions taken in a system were required to be recorded on a blockchain, it would provide a comprehensive audit trail that would aid intrusion investigation and forensics. Finally, blockchains can help improve the availability and fault-tolerance of computing systems, although alternative technologies exist.[11]

[10] *See* Rebecca Smith, *Russian Hackers Reach U.S. Utility Control Rooms, Homeland Security Officials Say*, Wall Street Journal (2018), https://on.wsj.com/2mCMAM4

[11] Fault-tolerant computing technology has a pedigree of several decades. For an early survey, see Michael Barborak et al., *The consensus problem in fault-tolerant computing*, 25 ACM Computing Surveys (1993), https://dl.acm.org/citation.cfm?id=152612. This technology is widely deployed in the Internet industry for building online services. *E.g.* Laura Nolan, *Managing Critical State: Distributed Consensus for Reliability, in* Niall Murphy et al., *Site Reliability Engineering: How Google Runs Production Systems*, O'Reilly Media (2016), https://landing.google.com/sre/book/chapters/managing-critical-state.html

On the other hand, blockchain technology might also introduce new cybersecurity risks. Let me highlight one. Participants in a blockchain network tend to adopt the same or similar software platforms. This so-called monoculture means that a vulnerability in one part of the network is a vulnerability in all of them, leading to the potential for cascading, rather than localized, failures.

To summarize, blockchain technology brings potential benefits as well as risks to the cybersecurity of energy systems. It is not essential for achieving the foundational components of digital security, and policy makers should view it as one of several possible technical tools for addressing energy cybersecurity.

Thank you again for the opportunity to address blockchain technology and its implications for energy efficiency and cybersecurity at today's hearing. I look forward to your questions.