Science | DOI:10.1145/3213762 Logan Kugler

Why Cryptocurrencies Use So Much Energy—and What to Do About It

The electricity consumption of mining for cryptocurrencies is becoming a real concern. Here's what to do about it.

In recent months, bitcoin and other cryptocurrencies have plunged in value, yet the market capitalization for these digital currencies is still valued at hundreds of billions of dollars. That market cap has grown more than 20 times since last year, when the cryptocurrency boom began.

With bitcoin's booming popularity comes problems. Speculation in bitcoin and other cryptocurrencies is rampant. Scams abound, and plenty of initial coin offerings (ICOs) have overpromised or underdelivered spectacularly.

Through it all, the world has focused on how bitcoin and other cryptocurrencies could implode and go to zero—or make you rich—depending on who you ask. Yet another aspect to cryptocurrencies has not received as much attention.

A major issue that results from increased adoption has not been adequately addressed; they use a lot of energy. The "mining" process that creates bitcoin uses more energy than Serbia, says Digiconomist, a self-described "platform that provides in-depth analysis, opinions, and discussions with re-

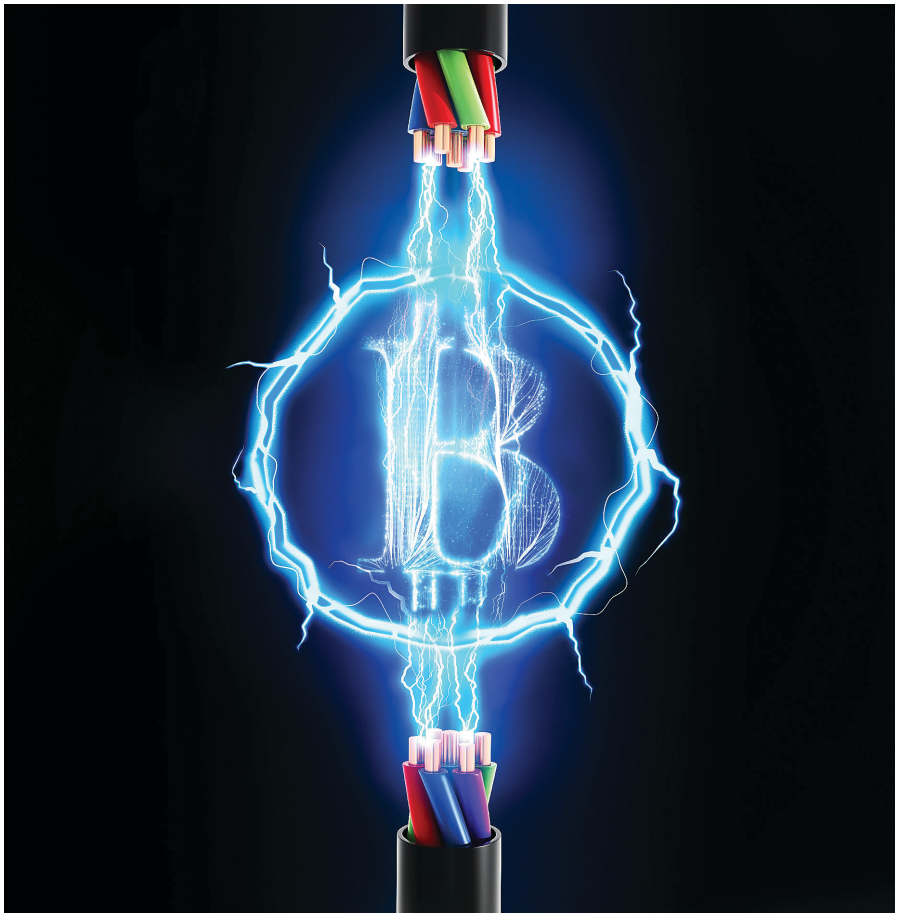

IMAGE BY ANDRIJ BORYS ASSOCIATES/SHUTTERSTOCK

gard to bitcoin and other cryptocurrencies ... on a voluntary, best-effort basis."

According to Bitcoinist, another industry site, the average cost in electricity to mine a bitcoin in Serbia is about $3,100, making it quite profitable to mine the coin there (among other countries with low-cost electricity).

As cryptocurrencies rise in price, the problem isn't going away. Right now, Digiconomist estimates that bitcoin mining, the process of generating bitcoins, accounts for 0.29% of the world's annual electricity consumption. The mining of a single bitcoin block—a block of tranasaction data on the bitcoin network—consumes enough energy to power more than 28 U.S. homes for a day.

Other cryptocurrencies that are structured similarly to bitcoin use energy for mining, too. Bitcoin is the most popular and best known cryptocurrency, but it is not unique in its energy needs.

Some people wonder if cryptocurrencies will disrupt the financial system, while others wonder if they will break the environment in the process.

Mining for Digital Gold

Many cryptocurrencies, including bitcoin, are "mined" into existence. Mining is when computers solve complex math problems to generate new bitcoins on the bitcoin network. The computers that solve each progressively more complex equation receive a reward in bitcoin.

According to site 99Bitcoins (a source of information on the crypto currency for the non-technical), a "constant amount" of bitcoins is created when a math problem is solved. The number of bitcoins awarded used to be 50 per problem solved, dispersed among all bitcoin miners; however, that number drops by half every 210,000 times an award is given out. In late 2017, that meant 12.5 bitcoins were awarded each time each progressively more difficult math problem was solved.

The bitcoin network, says the site, "is designed to produce a constant amount of bitcoin every 10 minutes." That means every time a miner joins the network, it will become harder to solve the problem resulting in the reward of bitcoins. The difficulty scales up to ensure bitcoin is generated every 10 minutes, no matter how much processing power you throw at it.

It is here that the energy problem arises. Bitcoin uses a "proof-of-work" (PoW) system to mine new bitcoins and verify transactions on the network. PoW means that computers "mining" bitcoin prove the data in each block of bitcoin being mined (the hard math problem to solve).

"The proof-of-work scheme requires guessing the solution to an equation (actually, an inequality)," says David Malone, a lecturer at Ireland's Maynooth University. "The guessing uses lots of computing power and, consequently, electricity."

When PoW is completed, rewards are paid out in bitcoin. Depending on the price of bitcoin at any given time, you may spend less in electricity costs than you receive in bitcoin, potentially making the venture profitable.

For instance, 99Bitcoins calculates that mining bitcoin for one month using one advanced piece of computer hardware would use 1,375kW of electricity, which it estimates would cost the user $118.

However, remember the part about the mining math problems getting harder over time? More and more computational firepower is required over time to mine at the same rate in order to keep your profitability stable, at least in terms of the number of bitcoins earned.

To cope, the bitcoin mining community often adopts ASICs, or application-specific integrated circuits. ASICs are circuits configured for a particular use case. Specialized ASICs are more powerful than regular computers at bitcoin mining, giving miners with these ASICs the ability to mine faster.

"Bitcoin's proof-of-work scheme has proven particularly easy to build custom hardware like ASICs for," says Malone. This has led to the adoption of custom—and energy-intensive—hardware by those who would mine bitcoins for profit.

The mining of a single bitcoin block consumes enough electricity to power more than 28 U.S. homes for a full day.

This isn't always the case with other cryptocurrencies.

"Some other proof-of-work schemes [known as being ASIC-resistant] are designed to be best calculated by regular computers, so people mining them can use regular computers instead of ASICs," says Malone.

The result is a vicious cycle, with the potential to consume an increasing amount of electricity.

More and more computing power is needed to mine bitcoin, which requires more and more electricity. ASICs can be used to supercharge your mining, which uses even more electricity, and if bitcoin's price rises, it becomes even more profitable to mine, which causes more miners to jump into the game. The more miners, the more computing power needed to crack bitcoin's math problems.

And so the cycle begins anew.

"So, while the value of bitcoin is higher than the cost of electricity, we can only expect more people to jump in, increasing the overall energy demands," says Malone.

How to Go Crypto-Green?

Bitcoin is the most popular cryptocurrency that uses PoW, but it's not the only one. Many cryptos run on various types of PoW schemes. Ethereum, one of the three most popular cryptos, uses a PoW scheme.

Bitcoin alone uses a lot of electricity, but should other PoW cryptos become popular, the problem could get much worse, much faster.

The good news is that the cryptocurrency community is aware of the problem, although possible solutions span the spectrum from theoretical to practical.

"Some systems use a semi-centralized model (like Ripple or Stellar) that are more green, but the trust assumptions are different than a fully decentralized system like bitcoin," says Joseph Bonneau, a cryptographer and assistant professor of computer science at New York University who used to work at Google.

These systems may circumvent the energy consumption concerns that arise with bitcoin, but may offer something fundamentally different from the value propositions of existing PoW cryptos.

Though cryptos like Ethereum use PoW, says Bonneau, some people might argue for it being a greener option, since Ethereum mining is typically performed on general-purpose graphics processing units (GPUs) that you can find in everyday computers. These are, theoretically, "greener because the hardware could be repurposed for other things if the currency dies out," Bonneau says. Bitcoin mining's specialized ASICs, on the other hand, would have zero practical value if bitcoin disappeared tomorrow.

Yet the real problem is the mining process itself, no matter how green it gets. Bitcoin and other PoW mining schemes are incentivized to consume energy.

"Bitcoin is currently valuable, so people want to earn bitcoins," says Malone. Miners use their computing power to add blocks of transaction data to the bitcoin blockchain; miners that do so are rewarded with more bitcoins.

"The way to earn bitcoins is to take part in adding blocks to the blockchain, as the bitcoin designers decided to reward this activity to incentivize people to maintain the blockchain," says Bonneau

He explains that cryptocurrency mining is "difficult by design to ensure that blocks are found at a certain rate, and money is created at a certain rate. If you designed a new chip that was twice as efficient, the puzzles would simply become twice as hard and there would be no benefit."

Mining, at the end of the day, is the work that ends up consuming most of the energy on any given crypto network.

In the case of bitcoin, says Bonneau, the energy costs are related "almost entirely to mining; that is, to solving computational puzzles. There are other energy costs of the system, like maintaining the system history, broadcasting and verifying new transactions, but those energy costs are trivial compared to the mining."

Some cryptocurrency developers have tried to circumvent the mining process entirely. They use a system called "proof-of-stake." These cryptocurrencies, which include DASH and PIVX, don't use PoW at all since it consumes too much energy, says Malone. Instead, users lock up quantities of cryptocurrency for periods of time, which secures the blockchain used by that currency. In return, they receive cryptocurrency rewards, as if they had mined cryptocurrency themselves.

No matter how green the mining process gets, cryptocurrencies based on proof-of-work schemes are incentivized to consume energy.

The result is, potentially, a middle path: cryptocurrency projects can still incentivize people to secure their networks, without requiring the energy needs of a small country to do so. C

Further Reading

Beigel, O.
Is Bitcoin Mining Profitable in 2018?, *99Bitcoins*, Jan. 2, 2018, https://99bitcoins.com/bitcoin-mining-profitable-beginners-explanation/

Bitcoin Energy Consumption Index, *Digiconomist*, https://digiconomist.net/bitcoin-energy-consumption

Rodgers, A.
The Hard Math Behind Bitcoin's Global Warming Problem, *WIRED*, Dec. 15, 2017, https://www.wired.com/story/bitcoin-global-warming/

Sompolinsky, Y. and Zohar, A.
Bitcoin's Underlying Incentives *Communications*, March 2018 https://cacm.acm.org/magazines/2018/3/225472-bitcoins-underlying-incentives/fulltext

Logan Kugler is a freelance technology writer based in Tampa, FL. He has written for over 60 major publications.

ACM Member News

COMBINING SIMULATIONS WITH REAL-TIME DATA

"My career has been focused on the problem of parallel and distributed execution of simulations," says Richard Fujimoto, Regents Professor at the School of Computational Science & Engineering of the Georgia Institute of Technology (Georgia Tech).

Fujimoto earned his master's degree and doctorate in Computer Science and Electrical Engineering from the University of California, Berkeley. He received two separate bachelor degrees, one in computer science, the other in computer engineering, from the University of Illinois, Urbana-Champaign.

His Ph.D. training began with an emphasis on computer hardware and architecture. During his studies, Fujimoto became interested in creating simulations and modeling. He has been more focused on software methods ever since, particularly on executing event simulations on parallel computers.

Fujimoto worked at the University of Utah for several years before joining Georgia Tech in 1989.

Much of his work now concerns combining simulations with real-time data. He describes using live data streams of traffic conditions to drive simulation models, which then make predictions about future conditions.

One area in which Fujimoto is particularly interested is mobile computing devices, particularly with regard to the amount of energy consumed by simulation computation, which affects battery life. He anticipates putting considerable effort into research on the energy consumption properties of distributed simulation algorithms on mobile devices.

Fujimoto also is passionate about promoting the stature of modeling simulation as a field in its own right, instead of merely as an application area.

—John Delaney