Powering down Bitcoin with silicon photonics: Researchers develop low power Bitcoin algorithm and hardware

May 4 2020, by Michael Dubrovsky, Lucianna Kiffer, Bogdan Penkovsky

Photonic miner prototype. Credit: PoWx.org

The island of Yap in Micronesia is known for its stone money called Rai.

The natives carved disks of limestone up to 4 meters (13 feet) in diameter at nearby islands and precariously transported them home. The stones were much too heavy to move repeatedly, and once on the home island, the Yapese devised an oral ledger to keep track of ownership as money changed hands in exchange for goods and services. The stones had no utility, but they were a trivially verifiable proof of resources expended and served for hundreds of years as a hard currency.

In the modern day, cryptographic proofs of work (PoW) became the cornerstone of the global decentralized currency known as Bitcoin. The fundamental innovation that differentiates proofs of work from physical embodiment of expended resources like Rai is that once a cryptographic "coin" is produced, the verification can be done computationally, allowing the proofs to be broadcast electronically with infinite copies for anyone to verify and store digitally. We admit that the analogy with coins is rather distant in this case.

Bitcoin's architecture was the first to succeed at getting a distributed network of computers to agree on a historical ledger of transactions without having a central authority/server acting as the "bank." Bitcoin "miners" compile the history of transactions and generate proofs of work to vote on the valid version. To encourage people to dedicate computing resources and electricity to generating those proofs, Bitcoins are minted and paid to the voters that are in the honest majority. The economic and game theoretic incentives turned out to be so robust that Bitcoin has never had a dishonest majority.

As Bitcoin gained utility and value over the last 10 years, the network incentivized billions of dollars in mining equipment and electricity expenditures. With the growth of the ecosystem, mining at home became unprofitable. Even the most expensive, cutting edge, special-purpose mining chip doesn't cover its energy costs unless you have direct access to very cheap electricity.

Yap stone money, with logs for carrying them Credit: "String Figures and How To Make Them", Caroline Furness Jayne, 1908, Wikimedia Commons / public domain

As we write this, the Bitcoin network is computing about 10^{20} SHA256 hashes per second, which is the bulk of the computation in Bitcoin's proofs of work. Every 10 minutes, the Bitcoin network computes as many hashes as there are stars in the universe! This is estimated to consume over 75 terawatt-hours per year, more than the electricity consumption of Austria (compared to 273 terawatt-hours for data centers worldwide). The consumption is growing by design as Bitcoin stores more value and in turn requires more security. Because miners are rewarded in Bitcoin for the proofs they generate, the reward's dollar value fluctuates with Bitcoin's market value. As the Bitcoin network's dollar value has grown about five orders of magnitude over the previous decade, so has the mining activity. Not only is this skyrocketing energy use an environmental concern, but it also threatens to compromise the very stability of Bitcoin as mining has centralized into a small number of massive data centers.

To decentralize Bitcoin mining once more and eliminate its massive electricity consumption, a proof of work decoupled from energy-intensive computation is clearly needed. We set out to design one that could be solved by photonic computing devices currently being commercialized as ultra-efficient deep learning accelerators. Shifting to this hardware paradigm would change the cost structure of mining. At the moment, proofs of work in Bitcoin are essentially proofs of electricity consumption as the cost of Bitcoin mining dedicated hardware is small compared to their lifetime electricity consumption cost.

In the case of a proof of work hosting a photonic accelerator, the major cost would be the capital expense of acquiring the hardware making it a Proof of hardware operation. This would even make possible home mining in urban areas due to decreased electricity costs. We also anticipate that fanless optical mining hardware will be possible due to decreased heat flux.

Photonic AI accelerators such as those being commercialized by Luminous, Lightelligence, Lightmatter and others promise to cut the energy use for matrix multiplications, measured in Joules per multiply and accumulate (MAC) operation, by several orders of magnitude. Naively, the way to design a proof of work compatible with such photonic accelerators would be to build a new hash that is based on MACs and use it in place of SHA256 in the proof of work cryptographic construction. In fact, R. Pappu's MIT thesis *Physical One Way Functions* was the original inspiration for using optics to replace digital processors for proof of work. However, we chose a different route to avoid the risk and complexity of designing a new hash. Typically, new hashes are associated with increased cryptographic security risks and as such are not deployed in mission-critical systems.

Novel optical proof of work (oPoW) is based on a hybrid cryptographic construction called Heavy Hash. Heavy Hash uses a proven digital hash (SHA256) to package a large amount of MAC computation into a proof-of-work puzzle. Heavy Hash can be computed on any standard digital hardware, but it becomes super-efficient only when a small digital processor is combined with a low-power photonic co-processor. For a more in-depth explanation, see this CES conference paper or check out the accompanying talk on YouTube.

You may ask: If digital hashing is still part of the Heavy Hash, how would oPoW reduce the hashrate if the digital components still need cooling and thus provide no efficiency gain? To give an example, an industry-standard all-digital dedicated hardware chip for Bitcoin mining is crammed with SHA cores running at the maximum clock rate allowed by the limits of heat dissipation. On the other hand, an oPoW miner would have a small digital core flip-chipped onto a large, low-power photonic chip and bottlenecked by the clock rate of the digital-to-analog and analog-to-digital converters. A cost comparable oPoW miner will have a much lower nominal hashrate (hashes/second) but each hash will correspond to proportionally more computation—hence the name Heavy Hash.

Photonics accelerators are made by fabricating waveguides in silicon using standard lithography processes. Silicon is transparent to infrared light and can act as a tiny on-chip fiber optical cable. Silicon photonics found its first use during the 2000s in transceivers for sending and receiving optical signals via fiber and has advanced tremendously over the last decade. One important difference between silicon electronics and silicon photonics is that due to the large de Broglie wavelength of photons as compared to electrons, there is no benefit to using the small feature sizes (5 nm) available for modern transistor fabrication. This means that the cost of commercializing a cutting-edge photonics product is an order of magnitude lower, because it can be done using less precise equipment. This is important, because access to advanced transistor manufacturing is very centralized (few foundries in the world).

Photonic miner setup: The Raspberry Pi communicates with the Qontrol controller via USB, which in turn is connected to the printed circuit board which carries the chip and transimpedance amplifiers. Wiring excluded. Credit: PoWx.org

By encoding a vector into optical intensities passing through a series of parallel waveguides, interfering these signals in a mesh of tunable interferometers (acting as matrix coefficients) and then detecting the output using on-chip Germanium photodetectors, a matrix-vector multiplication is achieved. A generalized discussion of matrix multiplication setups using photonics/interference can be found in Reck et al. and Russell et al. A detailed discussion of several integrated photonic architectures for matrix multiplication and corresponding tuning algorithms can be found in Pai et al.

For a practical demonstration, we designed and fabricated a prototype photonic miner (Figure 2). We ran a fork of the Bitcoin source code adjusted for optical proof of work on a Raspberry Pi board, which outsources matrix-vector multiplication to the photonic coprocessor (Figure 3).

We plan to open source the codebase, as well as our designs for the SiPh chip. We have also drafted a Bitcoin Improvement Proposal. The optical proof of work has potential for eventual adoption by the Bitcoin network. Additionally, we are continuing to optimize the photonic processors.

This story is part of Science X Dialog*, where researchers can report findings from their published research articles.* Visit this page *for information about ScienceX Dialog and how to participate.*

More information: Michael Dubrovsky et al., Towards Optical Proof of Work, CryptoEconSys Proceedings (2020). assets.pubpub.org/xi9h9rps/01581688887859.pdf

Bio:
Michael is a co-founder of PoWx, a non-profit dedicated to developing oPoW, as well as SiPhox, a stealth silicon photonics startup commercializing a next-generation silicon photonics manufacturing approach. He previously co-founded Simply Grid, which was acquired. He is currently a Fellow in the Advanced Study Program at MIT where he conducts research in the Materials for Micro and Nano Systems group, and was previously a Visiting Researcher at Technion University in the Materials Department and holds a B.S. in Chemistry from ESF/Syracuse University.

Citation: Powering down Bitcoin with silicon photonics: Researchers develop low power Bitcoin algorithm and hardware (2020, May 4) retrieved 17 May 2025 from https://sciencex.com/news/2020-05-powering-bitcoin-silicon-photonics-power.html