```
BIP: 52
Layer: Consensus (hard fork)
Title: Durable, Low Energy Bitcoin PoW
Author: Michael Dubrovsky <mike+bip@powx.org>
        Bogdan Penkovsky <bogdan+bip@powx.org>
Comments-Summary: No comments yet.
Comments-URI: https://github.com/bitcoin/bips/wiki/Comments:BIP-0052
Status: Draft
Type: Standards Track
Created: 2021-05-13
License: BSD-2-Clause
         OPL
```

Simple Summary

Bitcoin's energy consumption is growing with its value (see Figure below). Although scaling PoW is necessary to maintain the security of the network, reliance on massive energy consumption has scaling drawbacks and leads to mining centralization. A major consequence of the central role of local electricity cost in mining is that today, most existing and potential participants in the Bitcoin network cannot profitably mine Bitcoin even if they have the capital to invest in mining hardware. From a practical perspective, Bitcoin adoption by companies like Tesla (which recently rescinded its acceptance of Bitcoin as payment) has been hampered by its massive energy consumption and perceived environmental impact.

Figure. Bitcoin price and estimated Bitcoin energy consumption. Data sources: Cambridge Bitcoin Electricity Consumption Index, CoinDesk.

We propose a novel proof-of-work paradigm for Bitcoin--Optical proof-of-work. It is designed to decouple Bitcoin mining from energy and make it feasible outside of regions with low electricity costs. *Optical proof-of-work* (oPoW) is a modification of Hashcash that is most efficiently computed using a new class of photonic processors. Without compromising the cryptographic or game-theoretical security of Hashcash, oPoW shifts the operating expenses of mining (OPEX), to capital expenses (CAPEX)--i.e. electricity to hardware. oPoW makes it possible for billions of new miners to enter the market simply by investing in a low-energy photonic miner. Shifting to a high-CAPEX PoW has the added benefit of making the hashrate resilient to Bitcoin's price fluctuations - once low-OPEX hardware is operating there is no reason to shut it down even if the value of mining rewards diminishes. oPoW is hardware-compatible with GPUs, FPGAs, and ASICs meaning that a transitional period of optical and traditional hardware mining in parallel on the network is feasible

More information is available here: 1.

Abstract

As Bitcoin gained utility and value over the preceding decade, the network incentivized the purchase of billions of dollars in mining equipment and electricity. With the growth of competition, home mining became unprofitable. Even the most sophisticated special-purpose hardware (ASIC miners) doesn't cover its energy costs unless the miner also has direct access to very cheap electricity. This heavy reliance on energy makes it difficult for new miners to enter the market and leads to hashrate instability as miners shut off their machines when the price of Bitcoin falls. Additionally as the network stores ever more value, the percentage of world energy consumption that is associated with Bitcoin continues to grow, creating the potential for scaling failure and a general backlash. To ensure that Bitcoin can continue scaling and reach its full potential as a world currency and store of value, we propose a low-energy proof-of-work paradigm for Bitcoin. *Optical proof of work (oPoW)* is designed to decouple Bitcoin's security from massive energy use and make bitcoin mining feasible outside of regions with low electricity costs. *Optical proof-of-work* is a modification of Hashcash that is most efficiently computed using a new class of photonic processors that has emerged as a leading solution for ultra-low energy computing over the last 5 years. oPoW shifts the operating expenses of mining (OPEX), to capital expenses (CAPEX)–i.e. electricity to hardware, without compromising the cryptographic or game-theoretical security of Hashcash. We provide an example implementation of oPoW, briefly discuss its cryptographic construction as well as the working principle of photonic processors. Additionally, we outline the potential benefits of oPoW to the bitcoin network, including geographic decentralization and democratization of mining as well as hashrate resilience to price fluctuations.

Copyright

Motivation

As Bitcoin has grown over the past decade from a small network run by hobbyists to a global currency, the underlying Proof of Work protocol has not been updated. Initially pitched as a global decentralized network ("one CPU-one vote"), Bitcoin transactions today are secured by a small group of corporate entities. In practice, it is only feasible for entities that can secure access to abundant, inexpensive energy. The economics of mining limit profitability to places like Iceland, Texas, or Western China. Besides the negative environmental externalities, which may be significant, mining today is performed primarily with the consent (and in many cases, partnership) of large public utilities and the governments that control them. Although this may not be a problem in the short term, in the long term it stands to erode the censorship resistance and security of Bitcoin and other public blockchains through potential regulation or partitioning attacks.

Recent events, such as the ~25% hashrate crash due to coal-powered grid failure in china and Tesla's rescinding of its acceptance of Bitcoin as a form of payment, show that there are practical real-world downsides to Proof of Works's massive reliance on energy.

Whether or not the Bitcoin community accepts this common criticism as entirely valid, it has real-world effects which will only get worse over time. Eliminating the exponentially growing energy use currently built into Bitcoin without eliminating the security of PoW would be ideal and should not be a partisan issue.

New consensus mechanisms have been proposed as a means of securing cryptocurrencies whilst reducing energy cost, such as various forms of Proof of Stake and Proof of Space-Time. While many of these alternative mechanisms offer compelling guarantees, they generally require new security assumptions, which have not been stress-tested by live deployments at any adequate scale. Consequently, we still have relatively little empirical understanding of their safety. Completely changing the Bitcoin paradigm is likely to introduce new unforeseen problems. We believe that the major issues discussed above can be resolved by improving rather than eliminating Bitcoin's fundamental security layer—Proof of Work. Instead of devising a new consensus architecture to fix these issues, it is sufficient to shift the economics of PoW. The financial cost imposed on miners need not be primarily composed of electricity. The situation can be significantly improved by reducing the operating expense (OPEX)—energy—as a major mining component. Then, by shifting the cost towards capital expense (CAPEX)—mining hardware—the dynamics of the mining ecosystem becomes much less dependent on electricity prices, and much less electricity is consumed as a whole.

Moreover, a reduction in energy consumption automatically leads to geographically distributed mining, as mining becomes profitable even in regions with expensive electricity. Additionally, lower energy consumption will eliminate heating issues experienced by today's mining operations, which will further decrease operating cost as well as noise associated with fans and cooling systems. All of this means that individuals and smaller entities would be able to enter the mining ecosystem simply for the cost of a miner, without first gaining access to cheap energy or a dedicated, temperature-controlled data center. To a degree, memory-hard PoW schemes like Cuckoo Cycle, which increase the use of SRAM in lieu of pure computation, push the CAPEX/OPEX ratio in the right direction by occupying ASIC chip area with memory. To maximize the CAPEX to OPEX ratio of the Optical Proof of Work algorithm, we developed *HeavyHash* [1]. HeavyHash is a cryptographic construction that takes the place of SHA256 in Hashcash. Our algorithm is hardware-compatible with ultra-energy-efficient photonic co-processors that have been developed for machine learning hardware accelerators.

HeavyHash uses a proven digital hash (SHA3) packaged with a large amount of MAC (Multiply-and-Accumulate) computation into a Proof of Work puzzle. Although HeavyHash can be computed on any standard digital hardware, it becomes hardware efficient only when a small digital core is combined with a low-power photonic co-processor for performing MAC operations. oPoW mining machines will have a small digital core flip-chipped onto a large, low-power photonic chip. This core will be bottlenecked by the throughput of the digital to analog and analog to digital converters. A prototype of such analogue optical matrix multiplier can be seen in the figure below.

Figure. TOP: Photonic Circuit Diagram, A. Laser input (1550nm, common telecom wavelength) B. Metal pads for controlling modulators to transduce electrical data to optical C. Metal pads for tuning mesh of directional couplers D. Optical signal exits here containing the results of the computation and is output to fibers via a grating coupler the terminus of each waveguide. E. Alignment circuit for aligning fiber coupling stage. Bottom: a photograph of a bare oPoW miner prototype chip before wire and fiber bonding. On the right side of the die are test structures (F).

The *HeavyHash* derives its name from the fact that it is bloated or weighted with additional computation. This means that a cost comparable oPoW miner will have a much lower nominal hashrate compared to a Bitcoin ASIC (HeavyHashes/second vs. SHA256 Hashes/second in equivalent ASIC). We provide the cryptographic security argument of the HeavyHash function in Section 3 in Towards Optical Proof of Work [1]. In the article, we also provide a game-theoretic security argument for CAPEX-heavy PoW. For additional information, we recommend reading this article.

While traditional digital hardware relies on electrical currents, optical computing uses light as the basis for some of or all of its operations. Building on the development and commercialization of silicon photonic chips for telecom and datacom applications, modern photonic co-processors are silicon chips made using well-established and highly scalable silicon CMOS processes. However, unlike cutting edge electronics which require ever-smaller features (e.g. 5 nm), fabricated by exponentially more complex and expensive machinery, silicon photonics uses old fabrication nodes (90 nm). Due to the large de Broglie wavelength of photons, as compared to electrons, there is no benefit to using the small feature sizes. The result is that access to silicon photonic wafer fabrication is readily available, in contrast to the notoriously difficult process of accessing advanced nodes. Moreover, the overall cost of entry is lower as lithography masks for silicon photonics processes are an order of magnitude cheaper ($500k vs. $5M). Examples of companies developing optical processors for AI, which will be hardware-compatible with oPoW include Lightmatter, Lightelligence, Luminous, Intel, and other more recent entrants.

Specification

HeavyHash

The HeavyHash is performed in three stages:

1. Keccak hash
2. Matrix-vector multiplication
3. Keccak of the result xorred with the hashed input

Note that the most efficient matrix-vector multiplication is performed on a photonic miner. However, this linear algebra operation can be performed on any conventional computing hardware (CPU, GPU, etc.), therefore making the HeavyHash hardware-compatible with any digital device.

The algorithm's pseudo-code:

```
// M is a Matrix 64 x 64 of Unsigned 4 values

// 256-bitVector
x1 <- keccak(input)

// Reshape the obtained bitvector
// into a 64-vector of unsigned 4-bit values
x2 <- reshape(x1, 64)

// Perform a matrix-vector multiplication.
// The result is 64-vector of 14-bit unsigned.
x3 <- vector_matrix_mult(x2, M)

// Truncate all values to 4 most significant bits.
// This is due to the specifics of analog
// computing by the photonic accelerator.
// Obtain a 64-vector of 4-bit unsigned.
x4 <- truncate_to_msb(x3, 4)

// Interpret as a 256-bitvector
x5 <- flatten(x4)

// 256-bitVector
result <- keccak(xor(x5, x1))
```

Which in C can be implemented as:

```
static void heavyhash(const uint16_t matrix[64][64], void* pdata, size_t pdata_len, void* ou
{
    uint8_t hash_first[32] __attribute__((aligned(32)));
    uint8_t hash_second[32] __attribute__((aligned(32)));
    uint8_t hash_xored[32] __attribute__((aligned(32)));
    uint16_t vector[64] __attribute__((aligned(64)));
    uint16_t product[64] __attribute__((aligned(64)));

    sha3_256((uint8_t*) hash_first, 32, (const uint8_t*)pdata, pdata_len);

    for (int i = 0; i < 32; ++i) {
        vector[2*i] = (hash_first[i] >> 4);
        vector[2*i+1] = hash_first[i] & 0xF;
    }

    for (int i = 0; i < 64; ++i) {
        uint16_t sum = 0;
        for (int j = 0; j < 64; ++j) {
            sum += matrix[i][j] * vector[j];
        }
        product[i] = (sum >> 10);
    }

    for (int i = 0; i < 32; ++i) {
        hash_second[i] = (product[2*i] << 4) | (product[2*i+1]);
    }

    for (int i = 0; i < 32; ++i) {
        hash_xored[i] = hash_first[i] ^ hash_second[i];
    }
    sha3_256((uint8_t*)output, 32, (const uint8_t*)hash_xored, 32);
}
```

Random matrix generation

The random matrix M (which is a HeavyHash parameter) is obtained in a deterministic way and is changed every block. Matrix M coefficients are generated using a pseudo-random number generation algorithm (xoshiro) from the previous block header. If the matrix is not full rank, it is repeatedly generated again.

An example code to obtain the matrix M:

```
void generate_matrix(uint16_t matrix[64][64], struct xoshiro_state *state) {
    do {
        for (int i = 0; i < 64; ++i) {
            for (int j = 0; j < 64; j += 16) {
                uint64_t value = xoshiro_gen(state);
                for (int shift = 0; shift < 16; ++shift) {
                    matrix[i][j + shift] = (value >> (4*shift)) & 0xF;
                }
            }
        }
    } while (!is_full_rank(matrix));
}

static inline uint64_t xoshiro_gen(struct xoshiro_state *state) {
    const uint64_t result = rotl64(state->s[0] + state->s[3], 23) + state->s[0];

    const uint64_t t = state->s[1] << 17;

    state->s[2] ^= state->s[0];
    state->s[3] ^= state->s[1];
    state->s[1] ^= state->s[2];
    state->s[0] ^= state->s[3];

    state->s[2] ^= t;

    state->s[3] = rotl64(state->s[3], 45);

    return result;
}
```

Discussion

Geographic Distribution of Mining Relative to CAPEX-OPEX Ratio of Mining Costs

Below is a simple model showing several scenarios for the geographic distribution of mining activity relative to the CAPEX/OPEX ratio of the cost of operating a single piece of mining hardware. As the ratio of energy consumption to hardware cost decreases, geographic variations in energy cost cease to be a determining factor in miner distribution.

Underlying assumptions: 1. Electricity price y is fixed in time but varies geographically. 2. Every miner has access to the same hardware. 3. Each miner's budget is limited by both the cost of mining equipment as well as the local cost of the electricity they consume

budget = a(p+ey),

where a is the number of mining machines, p is the machine price, e is the total energy consumption over machine lifetime, and y is electricity price.

Note that in locations where mining is not profitable, hashrate is zero.

An interactive version of this diagram can be found here.

Why does CAPEX to OPEX shift lead to lower energy consumption?

A common misconception about oPoW is that it makes mining “cheaper” by enabling energy-efficient hardware. There is no impact on the dollar cost of mining a block, rather the mix of energy vs. hardware investment changes from about 50/50 to 10/90 or better. We discuss this at length and rigorously in our paper[1].

Working Principles of Photonic Processors

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.

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.

Below is a conceptual representation of a 3D-packaged oPoW mining chip. Note that the majority of the real estate and cost comes from the photonic die and the laser, with only a small digital SHA3 die needed (as opposed to a conventional miner of the same cost, which would have many copies of this die running in parallel).

Block Reward Considerations

Although it is out of the scope of this proposal, the authors strongly recommend the consideration of a change in the block reward schedule currently implemented in Bitcoin. There is no clear way to incentivize miners with transaction fees only, as has been successfully shown in On the Instability of Bitcoin Without the Block Reward and other publications, therefore looking a decade or two ahead it will be important to implement a fixed block reward or to slow the decay of the block reward to maintain the security of the network. Given that oPoW miners have low operating costs, once a large number of machines are running the reward level sufficient to keep them in operation and providing robust security can potentially be significantly smaller than in the case of the current SHA256 ASICs securing Bitcoin.

Implementation on the Bitcoin Network

A hard fork is not necessarily required for the Bitcoin network to test and eventually implement oPoW. It's possible to add oPoW as a dual PoW to Bitcoin as a soft fork. Tuning the parameters to ensure that, for example, 99.9% of the security budget would be earned by miners via the SHA256 Hashcash PoW and 0.1% via oPoW would create sufficient incentive for oPoW to be stress-tested and to incentivize the manufacture of dedicated oPoW miners. If this test is successful, the parameters can be tuned continuously over time, e.g. oPoW share doubling at every halving, such that oPoW accounts for some target percentage (up to 100% in a complete SHA256 phase-out).

Reverse compatibility Our understanding is that oPoW will not be reverse compatible.

ASICBOOST

Any new PoW algorithm carries the risk of hardware developers discovering and patenting an architecture with a significant speedup, as happened in the case of ASICBOOST for SHA256. HeavyHash is comprised of an SHA hash and 4-bit linear matrix-vector operations. The intent is for the matrix-vector multiplications to account for the majority of the work involved in computing a single HeavyHash operation. As we show in the Minimum Effective Hardness section of Towards Optical Proof of Work[1], there is no workaround to performing the matrix operations when computing HeavyHash, and since the SHA hashes are negligible, a true ASICBOOST-type speed up would require a speed up in linear matrix processing. Since matrix-vector multiplication is at the heart of neural networks and many other common computational workloads, it has been optimized very heavily and is generally very well understood. The acceleration of matrix-vector multiplication hardware (e.g. photonic coprocessors, memristors, etc.) is a very general problem and there are dozens of companies working on it, making it very unlikely for a single party to corner the market.

Endnotes

With significant progress in optical and analog matrix-vector-multiplication chipsets over the last year, we hope to demonstrate commercial low-energy mining on our network in the next 6 months. The current generation of optical matrix processors under development is expected to have 10x better energy consumption per MAC operation than digital implementations, and we expect this to improve by another order of magnitude in future generations.

PoWx will also be publishing the designs of the current optical miner prototypes in the near term under an open-source hardware license.

Acknowledgments

We thank all the members of the Bitcoin community who have already given us feedback over the last several years as well as others in the optical computing community and beyond that have given their input.

[1] M. Dubrovsky et al. Towards Optical Proof of Work, CES conference (2020) https://assets.pubpub.org/xi9h9rps/01581688887859.pdf

[2] https://sciencex.com/news/2020-05-powering-bitcoin-silicon-photonics-power.html

[3] KISS random number generator http://www.cse.yorku.ca/~oz/marsaglia-rng.html