Docket #: S22-139

LightHash: Photonic Blockchain Based on Optical Proof-of-Work

Stanford inventors have developed a framework that performs digitally verifiable photonic matrix-vector multiplication in integrated photonic networks, which may potentially enable energy-efficient hash functions and cryptocurrency mining. Bitcoin is estimated to consume 113 TWh annually, which is approximately 0.5% of the world's energy. Proposed programmable photonic networks are capable of energy-efficient matrix multiplication operations but are limited by their error, as cryptographic applications require 'consensus' – where several devices agree on a given computation. LightHash decreases systematic error and enables photonic consensus by minimizing bit error rate, such that the matrix operation operates in a limited space of possible outcomes that can be reliably reproduced across many devices. The algorithm is a slight modification of Bitcoin's proof of work, where LightHash achieves at least the same security guarantee.

Figure:

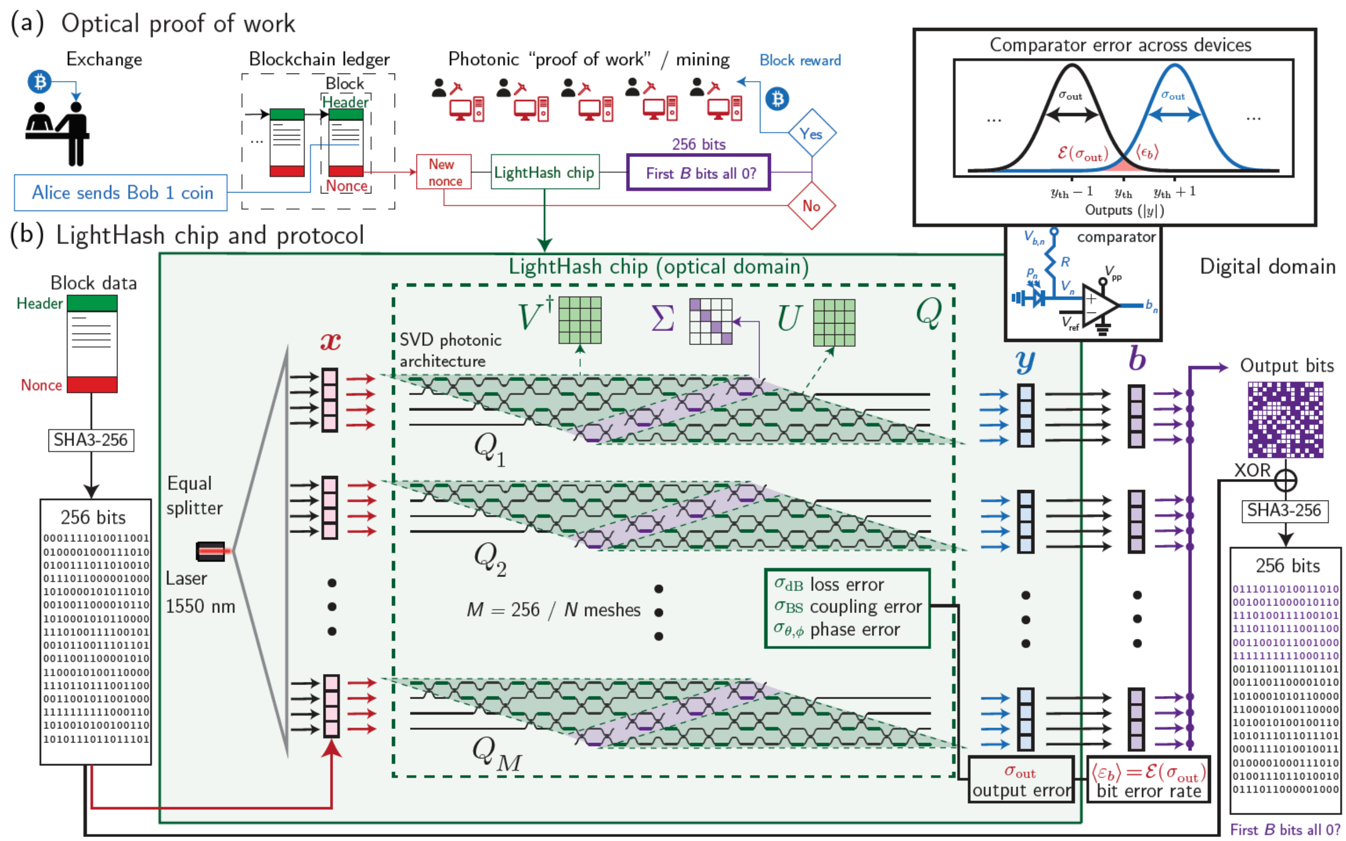

Figure Description: The LightHash protocol for optical proof of work - a) conceptual illustration and b) chip design.

Stage of Development

Prototype demonstrates that a photonic chip can implement a matrix-vector multiplication for a circuit size of 4. The inventors intend to implement LightHash for higher scalability.

Applications

- Decentralized blockchain applications
- Photonic cryptocurrency mining
- Photonic cryptography hardware solutions
- Photonic proof-of-work based spam filters and DDoS attack protection
- Digitally verifiable photonic computation
- Error-corrected photonic systems

Advantages

- Photonic integrated circuits accelerate computation and are more energy efficient
- Corrects systematic error in photonic matrix computation and preserves security guarantees

Publications

- Pai S, Park T, Ball M, Penkovsky B, Milanizadeh M, Dubrovsky M, Abebe N, Morichetti F, Melloni A, Fan S, Solgaard O, Miller DAB. Experimental evaluation of digitally-verifiable photonic computing for blockchain and cryptocurrency. arXiv 2022.
- Pai, S., Park, T., Penkovsky, B., Milanizadeh, M., Ball, M., Dubrovsky, M., ... & Miller, D. A. (2022, May). LightHash: Experimental Evaluation of a Photonic Cryptocurrency. In CLEO: Science and Innovations (pp. SF2K-2). Optica Publishing Group.

Innovators

- Sunil Pai
- David Miller
- Olav Solgaard
- Shanhui Fan
- Michael Dubrovsky
- Bogdan Penkovsky
- Marshall Ball

Licensing Contact

Luis Mejia

Senior Licensing Manager, Physical Sciences

Email