Exploring Green Cryptographic Hashing Algorithms for Eco-Friendly Blockchains

Aahad Abubaker
DePaul University
Chicago, IL, USA
aabubak2@depaul.edu

Tanmay Anand
Illinois Institute of Technology
Chicago, IL, USA
tanand4@hawk.iit.edu

Sonal Gaikwad
Illinois Institute of Technology
Chicago, IL, USA
sgaikwad4@hawk.iit.edu

Mahad Haider
Illinois Institute of Technology
Chicago, IL, USA
mhaider10@hawk.iit.edu

Jacklyn McAninch
Illinois Institute of Technology
Chicago, IL, USA
jmcaninch@hawk.iit.edu

Lan Nguyen
Illinois Institute of Technology
Chicago, IL, USA
lnguyen18@hawk.iit.edu

Alexandru Iulian Orhean
Illinois Institute of Technology
Chicago, IL, USA
aorhean@hawk.iit.edu

Ioan Raicu
Illinois Institute of Technology
Chicago, IL, USA
iraicu@iit.edu

Abstract

Cryptographic hash functions are fundamental for ensuring data security and integrity in all consensus algorithms in blockchains. While SHA256 has been widely used in many blockchain implementations, its throughput and efficiency has led the rise of a modern lightweight and speed superior implementation BLAKE3. We compared and contrasted SHA256 and BLAKE3 with a focus on blockchain workloads with small inputs and outputs. We explored different compilers and optimizations, different ways to parallelize using multi-threading and multi-processing, as well as different size systems from small Raspberry Pi 4 to a modern AMD Epyc server. We found that BLAKE3 is superior from a performance perspective. To showcase its strengths, we integrated BLAKE3 into a basic Proof-of-Space implementation that used advanced data index and search, and compared our results to the Chia blockchain plotting mechanism. Our approach offers one to two orders of magnitude higher hash generation and storage rates.

Keywords: Cryptographic hashing functions, SHA-256, BLAKE3, Blockchain, Bitcoin, Proof of Space and Time, Memoization, CryptoCurrency

1 Introduction

Blockchain technology is hailed as one of the most disruptive technological advancements of today. The architecture of blockchain technology is a decentralized and distributed ledger used to record transactions across a network of computers. The blocks in blockchain technology are securely held by cryptographic hashes, which encompass timestamps and transaction data from the previous block[1]. Hashing functions are referred to as one of the most important cryptographic primitives used in blockchain to ensure the integrity of data blocks for users. Hashing is defined as the process of transforming input data of arbitrary length into a fixed-length output message. The resulting string of data is called a hash, a hash code, or a message digest, while the input data is referred to as messages. A noteworthy facet of cryptographic hashes is that they make it impossible to convert the output message back into the input. This property enables cryptographic hashes to be a one-way function. Another interesting characteristic of cryptographic hashes is that they do not produce the same message digest for two different messages, thereby enhancing data integrity, data authentication, and security [2,3].

Most modern-day cryptocurrencies work on the Proof of Work consensus method, which consumes a high amount of electricity when adding new blocks to the blockchain. The proposed solution for this high power consumption blockchain network is a Proof of Space-based blockchain network that stores the number of hashes generated on storage devices and finds a winning hash from the pool of stored hashes.

The foundational building block of a new cryptocurrency based on the Proof of Space consensus method would be a high-throughput hashing function. We tested various hashing algorithms and conducted benchmarks for these modern functions, from small ARM-based devices such as the Raspberry Pi with 4 cores to large server clusters consisting of 8 sockets, each having 192 cores.

We conducted experiments and plotted a pool of hashes on storage devices. The results were fascinating, showcasing how our new CryptoMemoiz algorithm outperforms Chia coin's plotter. Our proposed methodology for hashing plots is also environmentally friendly, as we can achieve the same

SC'23, November 2023, Denver, CO, USA

throughput using low-power consumption hardware as we do with Chia coin's Madmax plotter on high-end server hardware.

2 Implementation

We wrote benchmarks to test Blake3 and SHA-256 in C. We conducted a thorough analysis of the performance of both hashing functions using various types of implementations, including multi-threaded code, GNU Parallel on the Linux shell, and MPI code. Additionally, we performed experiments by compiling the multi-threaded and MPI versions of the benchmark using two different compilers, GCC and CLANG. We observed a significant increase in performance when compiling our code with the CLANG compiler.

2.1 Hardware Used

For our experiments, we ran our hashing and subsequent plotting experiments on the following systems:

CPU Model	Sockets	Compute Power	RAM
Intel SP 8160	8	192c (384 HT) @ 2.1 GHz	768 GB
Intel HW 2620 v3	2	12c (24HT) @ 2.4 GHz	32GB
Intel Xeon Phi 7210	1	64c (256HT) @ 1.5 GHz	64GB
AMD Naples 7501	2	64c (128 HT) @ 2 GHz	128GB
Cortex-A72 (Pi)	1	4c (4 HT) @ 1.5 GHz	2 GB

2.2 Hashing Benchmarking Methodology

For our testing, our hash generation process consisted of the following when comparing the throughput and number of hashes generated by the hash functions, BLAKE3 and SHA-256.

We used two different compilers, GCC and Clang, to observe differences in throughput on our hashing benchmarks, gaining insights into how compiler choice impacts the hash generation speeds.

For parallel processing, GNU Parallel and OpenMPI benchmarking were used. We conducted a benchmarking study on multithreading capabilities using SHA-256 and BLAKE3 as hashing functions across various computing platforms, ranging from 1 to the maximum hardware threads of the respective machine.

2.3 Proof of Space Implementation

Using our knowledge of an optimized hash function and CryptoMemoiz' XSearch, we implemented BLAKE3 to our Proof of Space implementation, to which we generated benchmarks on the throughput of filling vaults with hashes using XSearch:

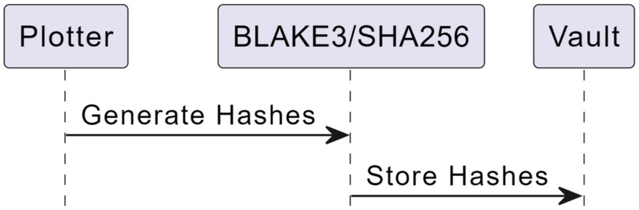

Figure 1. Hashing functions are used to generate hashes

3 Results

3.1 Benchmarking Results

The graphs above demonstrate BLAKE3's superior hash generation speed of 33.15 GB/s compared to SHA-256's mere 7.978 GB/s.

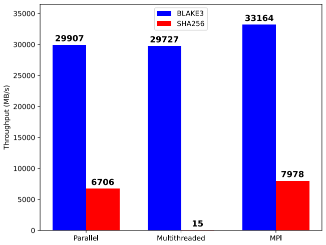

Figure 2. Hashing on 8Socket Machine ran at 384 HT

3.2 Proof of Space Plotting Results

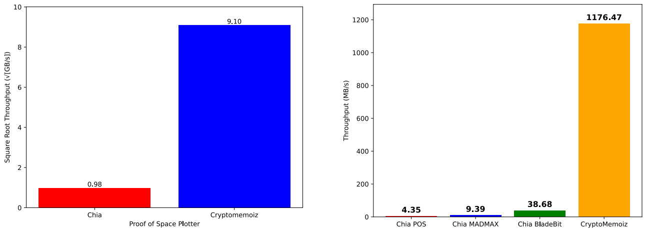

Figure 3. Plotting on Raspberry Pi

Figure 4. Plotting on AMD Naples 7501

Our successful integration of the optimized BLAKE3 function into CryptoMemoiz's proof of space implementation presents a significant breakthrough. The resulting plot generation performance surpasses the existing plotting mechanisms of the Chia blockchain, we got 1.38 MB/s speed for Chia plotter on a Raspberry Pi whereas using our plotter is 83 MB/s (Fig. 3). On server grade system i.e. AMD Naples 7501 we observed 1176 MB/s on CryptoMemoiz where Chia's bladebit plotter was only able to get 39 MB/s (Fig. 4), This achievement not only sets the stage for faster and more scalable plot creation but also aligns the aspiration for environmentally conscious and high-performance blockchain solutions.

References

[1] Buterin, V., et al. A next-generation smart contract and decentralized application platform. *white paper 3*, 37 (2014), 2–1.

[2] Cohen, B., and Pietrzak, K. The chia network blockchain. *vol 1* (2019), 1–44.

[3] Dziembowski, S., Faust, S., Kolmogorov, V., and Pietrzak, K. Proofs of space.

[4] Fleder, M., Kester, M. S., and Pillai, S. Bitcoin transaction graph analysis. *arXiv preprint arXiv:1502.01657* (2015).

[5] Gaži, P., Kiayias, A., and Zindros, D. Proof-of-stake sidechains. In *2019 IEEE Symposium on Security and Privacy (SP)* (2019), IEEE, pp. 139–156.

[6] Laurie, B., and Clayton, R. Proof-of-work proves not to work; version 0.2. In *Workshop on economics and information, security* (2004).

[7] Moran, T., and Orlov, I. Simple proofs of space-time and rational proofs of storage. In *Advances in Cryptology–CRYPTO 2019: 39th Annual International Cryptology Conference, Santa Barbara, CA, USA, August 18–22, 2019, Proceedings, Part I 39* (2019), Springer, pp. 381–409.

[8] Nakamoto, S. Bitcoin whitepaper. *URL: https://bitcoin. org/bitcoin. pdf-(: 17.07. 2019)* (2008).

[9] Orhean, A. I., Giannakou, A., Ramakrishnan, L., Chard, K., and Raicu, I. Scanns: Towards scalable and concurrent data indexing and searching in high-end computing system. In *2022 22nd IEEE International Symposium on Cluster, Cloud and Internet Computing (CCGrid)* (2022), pp. 51–60.

[10] Upton, E., and Halfacree, G. *Raspberry Pi user guide.* John Wiley & Sons, 2016.

[11] Vranken, H. Sustainability of bitcoin and blockchains. *Current opinion in environmental sustainability 28* (2017), 1–9.