Towards Eco-Friendly Cryptocurrencies: Optimizing Hashing Algorithms for Blockchain

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

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

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

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

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

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

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

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

Abstract

Cryptocurrencies have often been criticized for their environmental impact and sluggish transaction speeds, primarily due to compute-intensive consensus mechanisms like Proof of Work (PoW), as seen in Bitcoin. To address these challenges, our team has harnessed an alternative consensus mechanism, Proof of Space, coupled with the power of XSearch—a search engine-optimized library. This synergy has given rise to CryptoMemoiz: a pioneering Proof of Space (PoS) implementation that is capable of outperforming comparable cryptocurrencies, for example, Chia, in cryptocurrency plot generation. Notably, CryptoMemoiz excels in energy efficiency, functioning even on low-power devices like Raspberry Pis, thus democratizing cryptocurrency mining. Finally, CryptoMemoiz boasts multi-threaded plotting and asynchronous I/O for block writes, ensuring optimal CPU utilization during plot generation. Our solution's performance underscores its capacity to meet the technical requisites for widespread adoption and scalability.

Keywords: Cryptographic hashing functions, SHA-256, BLAKE3, blockchain, Bitcoin, Proof of space and time, Memoization, Cryptocurrency

1 Introduction

Blockchain technology is hailed to be one of the most disruptive technological advancements of today. The architecture of blockchain technology is a decentralized and distributed ledger that is used to record transactions across a network of computers. The blocks in the blockchain technology are securely held by cryptographic hashes, these hashes encompass timestamps and transaction data of the previous block[1]. Hashing functions is referred to as one of the most important crypto-primitives used in Blockchain to proffer integrity of data blocks to users. Hashing is defined as the process of transforming an input of arbitrary length data into a fixed-length of output message. The resulting string of data is called a hash or a hash code or a message digest whilst the input data is called messages. A noteworthy facet of cryptographic hashes is that they make it impossible for the output messages to be converted into input. This property enables cryptographic hashes to be one-way function. Another interesting characteristic of cryptographic hashes is that it does not produce the same message digest for two different messages, thereby proffering enhanced data integrity, data authentication and security[2,3]. Most modern day cryptocurrencies works on Proof of work consensus method, which consumes high amount of electricity for adding of new blocks in the blockchain, the proposed solution for this high power consumption blockchain network is a proof of space based blockchain network which stores the amount of hashes generated on storage devices and finds a winning hash from the pool of stored hashes.

Building block of a new cryptocurrency based on proof of space consensus method would be a high throughput hashing function. We tried a lot of hashing algorithms and ran benchmarks of these modern functions on small ARM based devices such as Raspberry Pi having 4 cores to huge server clusters consisting of 8 sockets having 192 Cores in it.

We did experiments and tried to plot pool of hashes on storage devices, we saw fascinating results on how our new CryptoMemoiz algorithm which consists of supersedes Chia coin's plotter.Our new proposed methodology for plotting hashes is also environment friendly as we can use low power

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

consumption hardware to plot hashes and get same throughput as we were getting for Chia coin's Madmax plotter on high end server hardware.

2 Implementation

We wrote benchmarks to test Blake3 and SHA-256 in C.We did a thorough analysis of the performance of both the hashing functions using various types of implementations like Multi threaded code, GNU Parallel on Linux shell and MPI code. We also did experiments by compiling the multi-threaded version and MPI version of the benchmark using two different compilers i.e. GCC and CLANG, we found a significant increase in the performance while compiling our code from 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.

Compilers, 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.

Parallel Processing and Multithreading, GNU Parallel and OpenMPI for parallel processing 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 768 threads.

2.3 Proof of Space Implementation

Using our knowledge of an optimized hash function, we implemented BLAKE3 to our Proof of Space implementation, to which we generated benchmarks on the throughput of filling vaults with hashes.

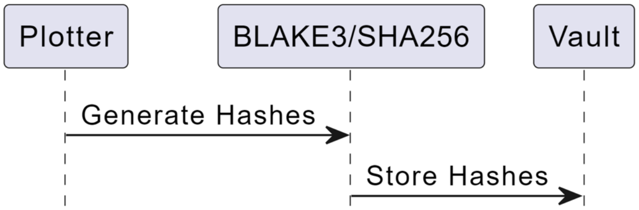

Figure 1. Hashing functions are used to generate hashes

3 Results

3.1 Benchmarking Results

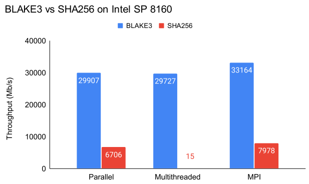

Figure 2. Hashing Performance on 8Socket Machine

- Each implementation was ran at the upper limit of 384 HT for the machine.

The above graphs showcase how BLAKE3 supersedes SHA-256 in generating hashes by generating 33.15 GB/s whereas SHA-256 can generate mere 7.978 GB/s.

3.2 Proof of Space Plotting Results

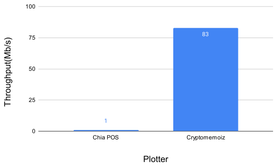

Figure 3. Plotting Performance on Raspberry Pi

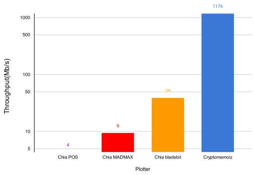

Figure 4. Plotting Performance on AMD Naples 7501

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

[4] 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.

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

[6] 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.

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

[8] 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.

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

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