Towards Eco-Friendly Cryptocurrencies: Optimizing Hashing Algorithms for Blockchain

Aahad Abubaker [1] Tanmay Anand [2] Sonal Gaikwad [2] Mahad Haider [2] Jacklyn McAninch [2]
Lan Nguyen [2] Alexandru Iulian Orhean [2] Ioan Raicu (Advisor) [2]

[1]DePaul University [2]Illinois Institute of Technology

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.

Background

- In the realm of blockchain technology, cryptographic hash functions are fundamental for ensuring data security and integrity. While SHA256 has been widely used, its throughput and efficiency have been scrutinized. BLAKE, a more advanced hash function, has emerged as a potential alternative with superior throughput.
- Blockchain's decentralized ledger system has revolutionized industries, but cryptocurrencies like Bitcoin, based on energy-intensive Proof of Work (PoW) consensus, have raised environmental concerns. The rise of Proof of Space, exemplified by Chia, offers an energy-efficient alternative, using storage instead of computation for consensus.
- Our research compares BLAKE and SHA256 throughput and explores Proof of Space's potential. By benchmarking hash functions and analyzing blockchain consensus mechanisms, we are able to implement findings to our implmentation of a Proof of Space consensus, CryptoMemoiz.

Machine Specifications

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

References

[1] Alexandru Iulian Orhean, Anna Giannakou, Lavanya Ramakrishnan, Kyle Chard, and Ioan Raicu. 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)*, pages 51–60, 2022. doi:10.1109/CCGrid54584.2022.00014.

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:** GNU Parallel and OpenMPI for parallel processing benchmarking were used.
- **Multithreading:** 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.
- **I/O Size:** To generate hashes, the input size will be 64 bytes and the output size will be 12 bytes.

Benchmarking Results

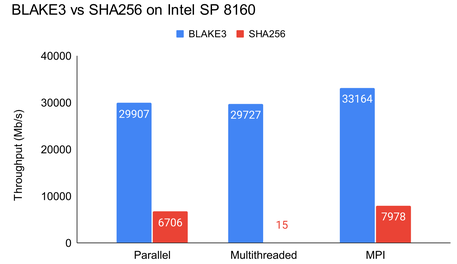

Figure 1. Hashing Performance on 8Socket Machine (Clang)

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

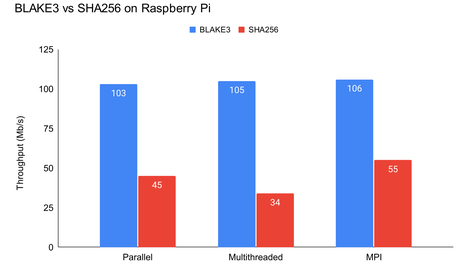

Figure 2. Hashing Performance on Raspberry Pi (Clang)

- Each implementation was ran at the upper limit of 4 HT for the machine.

MEMO

Following are some problems with the current leading blockchains that MEMO aims to address:

- **Low Throughput** Leading cryptocurrencies like Bitcoin can only handle around 5 transactions per second, which is significantly slower than centralized payment methods like Visa and Mastercard, which can handle around 20,000 transactions per second. We are trying to write a new blockchain using Google protocol buffers and ZeroMQ which will have high throughput.
- **High Carbon Emission** Bitcoin's energy-intensive proof-of-work consensus algorithm results in a massive carbon footprint of 458.46 kgCO2, which is equivalent to the carbon footprint of 1,016,111 Visa transactions or 76,410 hours of watching YouTube. MEMO being a proof of space coin is more environment friendly as it uses memoization to save the hashes instead of using GPUs or ASICs which consume high electricity.
- **Problems with Proof-of-Stake Approach** While Ethereum, the second most popular cryptocurrency in the world, has shifted from proof-of-work to proof-of-stake, the problem with the proof-of-stake validation method is that it can potentially centralize the network, as only a few people in the world may have enough money to become a validator. In MEMO we are using proof of space consensus method which keeps the distributed nature of the blockchain alive by keeping the network decentralised.

Proof of Space Work

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:

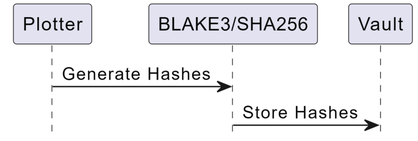

Figure 3. Plotting Performance on Epycbox

Proof of Space Results

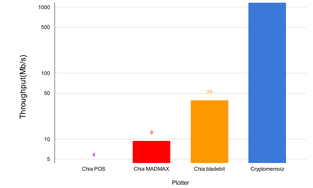

Figure 4. Plotting Performance on Epycbox

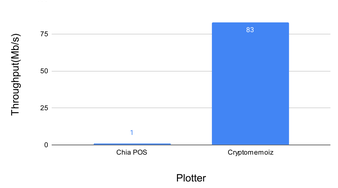

Figure 5. Plotting Performance on Raspberry Pi

Conclusions

- In summary, our comprehensive analysis conclusively establishes BLAKE3 as the superior choice for hash generation, especially when leveraged with advanced techniques like multithreading, parallel processing in GNU, and MPI.
- Furthermore, 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. 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.
- The seamless integration of the optimized BLAKE3 function into CryptoMemoiz heralds a new era of enhanced efficiency and sustainability in blockchain operations, establishing our solution as a compelling alternative that outperforms Chia's proof of space mechanism.

Acknowledgements

This work was supported in part by the National Science Foundation (NSF).