Improving Energy Efficiency of Ethereum Mining

[1]Siddhartha Sharma, [2]Jayash Kumar Sharma, [3]Arun Kumar Yadav
[1]M. Tech Research Scholar, [2,3]Associate Professor
[1,2,3]Department of Computer Science & Engineering,
[1,2]Hindustan Institute of Technology and Management, Agra, Uttar Pradesh, India
[3]ITM University Gwalior, Madhya Pradesh, India

Abstract: Ethereum is one of the most successful digital currencies and is continuously growing. With the increase in mining difficulty and huge energy requirements of it, it is becoming necessary to find efficient ways to increase the mining throughput without increasing energy requirements to mine cryptocurrency. Ethereum mining is much more heavily reliant upon graphic memory speeds than the actual core speed of the GPU itself which means that we can tune the graphics card for an efficient workload and don't have to run the GPU at high heat output core clocks that consume a lot of wattage in order to get a good mining session. To actually get the best hash rate we're going to test the GPUs with different memory configurations.

IndexTerms **- Ethereum, mining, efficiency.**

I. INTRODUCTION

Ethereum is a platform to build decentralized applications with blockchain technology. Bitcoin was the first blockchain application and Ethereum does to applications what bitcoin did for money, which is removing the need for a trusted third party. For the Bitcoin blockchain we had blocks and these blocks are just are just objects that store data. The blockchain is linked-list that is stored on everybody's computer and the Ethereum blockchain is very similar except it's different in what is stored in those blocks are not just transactions but also the code snippets and smart contracts. Ethereum is a programmable blockchain and has a refined scripting language.

What can be built on Ethereum is only limited by the creativity of their developers .That said, such technology has three types of applications that immediately comes to mind. The first are individual currencies. Imagine if you're an artist and you want to support yourself by issuing a brand new currency. If you want to support this artist, you could purchase that currency, technically investing in their own personal IPO. And as those millions of currencies are traded on decentralized exchanges currency itself becomes a representation of your values and not just a means of exchange. Ethereum makes it easy to issue our own tokens of value so we can reward our users for actions that they take even outside of the network, such asfoursquare check-ins.Retailers can issue crypto tokens of similar value instead of giving out loyalty points which then could be exchanged with services on currency wallets or exchanges or with other tokens like air miles.On a decentralized network, the need of a middleman is limited to bringing true value-add such as insurance for example, rather than just bringing two people closer for a Kickstarter campaign, giving out airdrops and early user adoption benefits is much more useful that giving out goodies and accessories, and users could be rewarded with tokens of value into the startups that they invest in.

In 2017, when Vice published an article [12], that Ethereum miningis already consuming energy resources more than a small country andthe Ethereum network in total could be using as much as 5 Terawatt-hours (TWh) of electricity each year while the Bitcoin network is consuming 32 TWh and is growing[11]. Ethereum uses smart contracts which can help build similar currencies While the Ethereum has a plan to move away from its current energy intensive mining algorithm with proof of stake, it is still few years away and with its programmable decentralized application the coins that are derived from Ethereum might not be able to take the advantage of it.

1.1 Theoretical framework

The Ethereum uses Ether (ETH) as its inbuilt currency which is used for paying for smart contracts to run. Ethereum store the data in IPFSas you don't want to store data directly in the block chain because it's too big and every miner has to download a copy of this blockchain and all the transactions and that includes code and whatever else is in those transactions, but if we're storing movies really big files in the blockchain these things are going to become too large to be feasible so the way it uses to fix that is to store it in a distributed hash table. What IPFS gives back is a hash a Content address for all of that content and that is what we store in the blockchain. The hash table get back the hash and store that hash in the block chain which then points to the data storage. Ethereum uses three Merkle trees to store transactions, receipts and states and is called a Patricia tree. Ethereum Virtual Machine calculates the elements which is responsible for contract logic. The peer to peer sharing swarm here is the storage layer and the whisper is used for encrypting the messaging protocol for all the nodes to be able to message each other and they both uses IPFS. Solidity, Serpent and LLL are the smart contract programming languages that are used. The popular Ethereum clients are geth which is written in Go and pyethapp for python.

II. PREVIOUS AND RELATED WORK

At the core of Ethereum, we have blockchain technology. If we look at centralized applications, we'll find that they reach trust by being closed firewalls and security teams that we have to trust, and trust to do their job well. Blockchain technology on the other hand uses a different model, one by which trust can be reached on an open network.[6]Bitcoin is a currency that was the first and currently most successful implementation of block chain technology Things that can be mathematically explained can be detailed, secured and traded and just like in bitcoin, where we do not need to trust into a bank or a central authority to keep our funds safe. On Ethereum, our personal information, our identity and our funds stay under our control at all times. In Ethereum there is business logic which is known as contracts. These contracts have a set of instructions that they follow every time they get a transaction message. Contracts can store data, send and receive transactions and even interact with other contracts independently of any control. They are maintained by the network and they are written in a programming language that will be instantly familiar to any developer. These Ethereum contracts are also decentralized, and does not require an infrastructure to setup and launch an application. This sharing network allows it to be impervious to DDOS attacks.

O Ala-Peijari proposed a method of using ASIC miners and compared the performance of FPGA calculations [4]. There are previous techniques proposed for mining bitcoin with the help of ASIC miners that are application specific integrated circuits used for specifically doing a single type of calculation. Ethereum algorithm on the other hand is ASIC resistant to keep a fair currency and avoid mining centralization [2]. Other users have tried and found out that the general purpose computation is heavily reliant on the memory clocks compared to the core clocks of the system [3].

Since most computation of Ethereum are general purpose calculation it is difficult to build an ASIC miner that will be better than current systems. Since ASIC can't keep up with ever increasing DAG (Directed Acyclic graph) file whichchanges after every 30000 block or roughly 100 hours.

III. Motivation

As the mining difficulty kept increasing [13] and with the global shortage of GPUs and their steep rise in price[14]. It has become inevitable to find alternative ways to improve on the current scenario in order to keep the mining cost in check. Due to a these factors we tried searching for an efficient method to mine coins because hard fork of proof of stake implementation is still in future and the current implementation only uses one stake validation after every 100 mined blocks.

3.1Proposed Method

Memory over clocking puts out only a little extra heat as opposed to the massive extra heat output that we get with core over clocking so there is less strain on the cards fans than if we over clock the core frequency here. We first tried to find out the optimal memory overclock for the system and tried various core clocks to reduce the energy consumption and then improved on the memory timing for every clock in order to get the most out of every GPU cycle improving the overall efficiency of the system.

IV. Research Methodology

The methodology section outline the plan and method that how the study is conducted. We are using an Nvidia GTX 1060 and an AMD RX480 GPU with claymore miner to compare the mining performance;

4.1Improving Memory Clocks

As we increased each of the memory clocks on each of the video cards, the hash rate definitely increases however when we kept the memory clock at the peak overclock of 600 megahertz and dropped the core clock by 400 megahertz the GTX 1060 lose roughly only half mega hash which is significantly less power consumption for roughly the same result.**[Fig.1]**

With AMD the core clock matters a bit more but there's still definitely value to be found in increasing the memory clock to increase the hash rate. We went from mid half mega hash dropping the core clock by 400 megahertz here in a slightly larger loss than with Nvidia but still very close to stock hashing rate for a 33% decrease in power consumption and is a sweet spot for optimal efficiency per watt to make the most money after electricity costs.**[Fig.2]**

4.2Improving Memory Timings

Modifying the BIOS on an NVIDIA GPU is not possible in Pascal generation, as they've encrypted their BIOS so there is no chance of changing them at the present. However, AMD hasn't encrypted their bios's on their Polaris GPUs. We extracted the bios and our primary focus will be to work on the VRAM timings to allow for the faster hash rate, what it does is allow us to have the memory run quicker at the same speed we were running before, which means a better performance for every clock. Tighter memory timings have given us more performance without spending too much extra power getting to higher mining rates specifically with this. We used the hex data of 1750 MHz timing cycle to improve the 2000 MHz cycle. After flashing the modded bios to our RX480 GPU we got a performance speed up of 27.91 MH/s at stock clocks on the modded bios compared to the 24.65 MH/s that we were getting before the BIOS flash at stock settings.

From here you can improved the memory clock as we discussed above in 4.1 and reached the mining speed of 30.28Mh/s**[Fig.3]** which is 22.8% higher than the original stock performance.

V. Results and Discussion

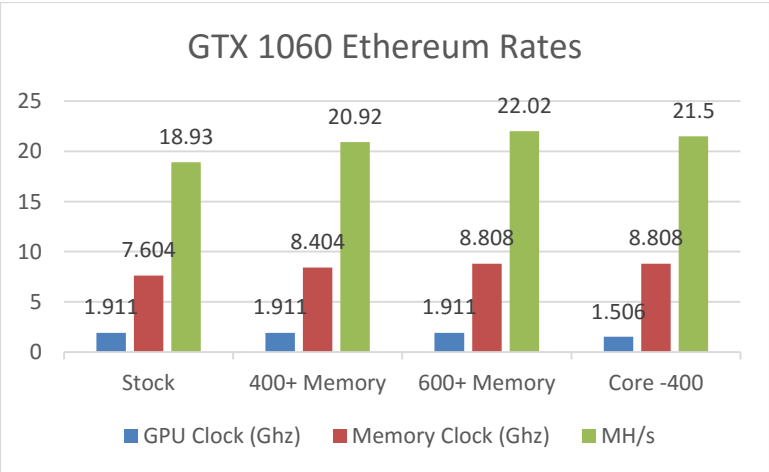

Figure 1 shows the mining Improvements in gtx 1060

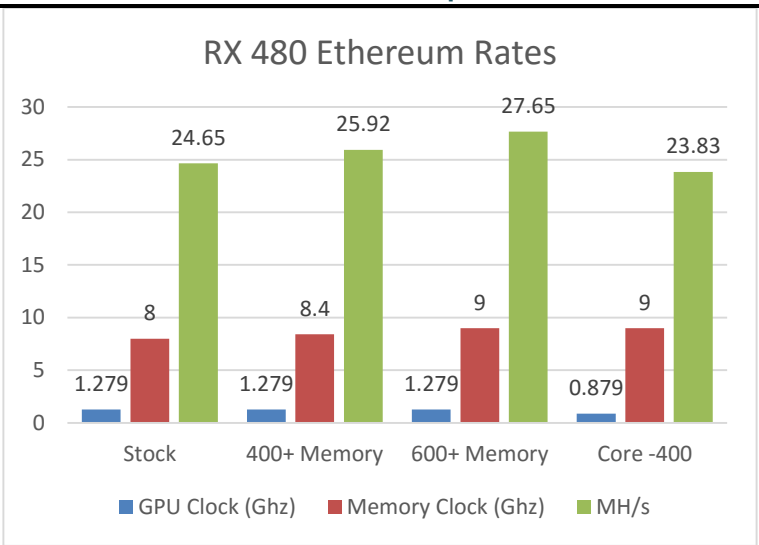

Figure 2 shows the mining improvements on RX 480

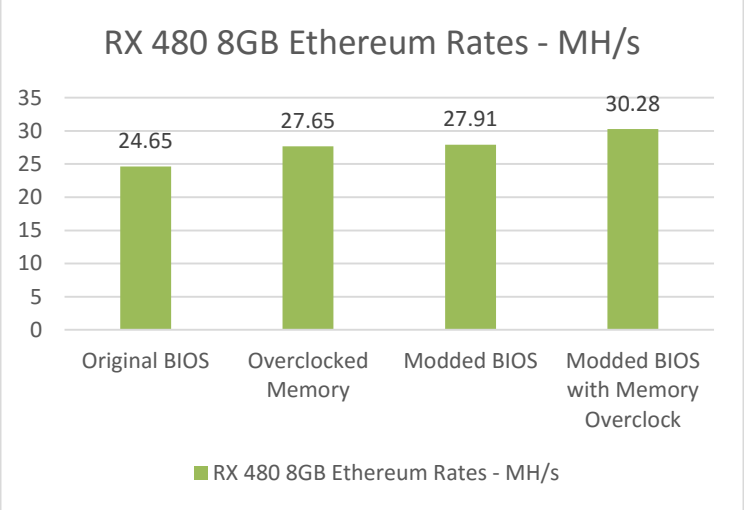

Figure 3 shows the improvements overtime on RX480

VI. Conclusion

In this paper we used a combination of tighter memory timing and overclock to achieve an optimal 22.8% improvement over the stock clocks with 8% of increased power consumption. It can further be improved with core overclocks but that will reduce the optimal price to performance ratio. We saw similar improvements for other alt coins like Monero and Ethereum derived ones. This can be further enhanced to use for other ICO that are developed with ether blockchain technology. Pairing multiple GPUs in a mining rig will give higher returns over the single card that we have tested here.

References

[1] AP Ozisik. 2017. Estimation of Miner Hash Rates and Consensus on Blockchainshttps://arxiv.org/pdf/1707.00082 (2017).
[2] Ethereum Whitepaperhttps://github.com/ethereum/wiki/wiki/White-Paper.
[3] https://ethereum.stackexchange.com/questions/16811/is-ethereum-asic-resistant
[4] OAla-Peijari.2014. Bitcoin the Virtual Currency: Energy Efficient Mining ofBitcoins.
[5] REM: Resource-Efficient Mining for Blockchains https://eprint.iacr.org/2017/179.pdf (2017).
[6] Satoshi Nakamoto. 2009. Bitcoin: A Peer-to-Peer Electronic Cash System. https://bitcoin.org/bitcoin.pdf. (May 2009).
[7] The Bitcoin Lightning Network: Scalable Off-Chain Instant Payments. https://lightning.network/lightning-network-paper.pdf.(July 2015)
[8] Ethereum. Ethereum Homestead Documentation. http://ethdocs.org/ en/latest/.
[9] Ethash. 2017. https://github.com/ethereum/wiki/wiki/Ethash. (Last retrieved June 2017)
[10] Bitcoin 2015. Confirmation. https://en.bitcoin.it/wiki/Confirmation. (February 2015).
[11] https://venturebeat.com/2018/02/25/the-real-cost-of-mining-ethereum/(2018)
[12] Ethereum Already using a Small Country's Worth of Electricity (2017) https://motherboard.vice.com/en_us/article/d3zn9a/ethereum-mining-transaction-electricity-consumption-bitcoin (2017)
[13] It is No Longer worth It to Build an Ethereum Mining Righthttps://motherboard.vice.com/en_us/article/nedn3d/ethereum-mining-rig-no-longer-worth-it (2017)
[14] Crypto Mining Craze Creates Global GPU Shortagehttps://www.newsbtc.com/2018/02/21/popularity-of-mining-has-created-a-worldwide-shortage-of-gpus/ (2018)