ANKARA YILDIRIM BEYAZIT UNIVERSITY

GRADUATE SCHOOL OF NATURAL AND APPLIED SCIENCES



COMPARISON AND OPTIMIZATION OF GPU PERFORMANCES ON ETHEREUM MINING

M.Sc. Thesis by

Gizem KIZILBEY

Department of Electrical and Electronics Engineering

September, 2019

ANKARA

COMPARISON AND OPTIMIZATION OF GPU PERFORMANCES ON ETHEREUM MINING

A Thesis Submitted to

The Graduate School of Natural and Applied Sciences of

Ankara Yıldırım Beyazıt University

In Partial Fulfillment of the Requirements for the Degree of Master of Science in Electrical and Electronics Engineering, Department of Electrical and Electronics Engineering

by

Gizem KIZILBEY

September, 2019

ANKARA

M.Sc. THESIS EXAMINATION RESULT FORM

We have read the thesis entitled **"COMPARISON AND OPTIMIZATION OF GPU PERFORMANCES ON ETHEREUM MINING"** completed by **GİZEM KIZILBEY** under the supervision of **PROF. DR. İLYAS ÇANKAYA** and we certify that in our opinion it is fully adequate, in scope and quality, as a thesis for the degree of Master of Science.

Prof. Dr. İlyas ÇANKAYA

Supervisor

Asst. Prof. Dr. Cemal KOÇAK

Jury Member

Asst. Prof. Dr. Hilal KAYA

Jury Member

Prof. Dr. Ergün ERASLAN

Director

Graduate School of Natural and Applied Sciences

ETHICAL DECLARATION

I hereby declare that, in this thesis which has been prepared in accordance with the Thesis Writing Manual of Graduate School of Natural and Applied Sciences,

- All data, information, and documents are obtained in the framework of academic and ethical rules,
- All information, documents, and assessments are presented in accordance with s scientific ethics and morals,
- All the materials that have been utilized are fully cited and referenced,
- No change has been made on the utilized materials,
- All the works presented are original,

and in any contrary case of the above statements, I accept to renounce all my legal rights.

Date: **Signature: ……..**

Name & Surname:…….

ACKNOWLEDGMENTS

Firstly, I would like to express my sincere gratitude to my supervisor, Prof. Dr. İlyas ÇANKAYA for his tremendous support and motivation during my study. His immense knowledge and precious recommendations constituted the milestones of this study. His guidance assisted me all the time in my research and while writing this thesis.

I wish to thank my parents Nursel & Metin KALKANCI and my brother Erkan KALKANCI and his wife Ulviye KALKANCI who have been with me in every period of my life and who have supported me. In addition, I would like to thank my loving and supportive husband Oğuzhan KIZILBEY.

2019, 19 September **Gizem KIZILBEY**

COMPARISON AND OPTIMIZATION OF GPU PERFORMANCES ON ETHEREUM MINING

ABSTRACT

Bitcoin, which emerged in 2008 with the article "Bitcoin: A Peer-to-Peer Electronic Cash System", is increasing its popularity day by day by adding new terms to scientific literature. Developed as an alternative cryptocurrency, Ethereum is a system that allows for anonymous and inexpensive asset transfer between the opposite ends without the need for a central server or a checkpoint. Bitcoin and alternative crypto coins are the most common use of blockchain structure. Crypto coins are realized by mining which is the solution of a challenging algorithm. Any miner in the system uses the graphics card and processor power in hand to obtain this solution. As the processors of the GPUs are more efficient in floating point calculations, the performances of the various graphics cards used in Ethereum mining will be focused on in this study. The model and memory quantities of the graphics cards used are as follows: 4 GB AMD R9 290, 4 GB AMD R9 380, 8 GB AMD R9 390, 4 GB AMD RX 560, 4 GB AMD RX 470, 4 GB AMD RX 480, 4 GB AMD RX 570, 4 GB AMD RX 580, 6 GB NVIDIA GTX1060, 8 GB NVIDIA GTX1070, 8 GB NVIDIA GTX1080. The most important aim of this study is to apply optimization methods in the Ethash summary algorithm which is specific for Ethereum mining. For this purpose, improvements have been made to enable AMD and NVIDIA chipset graphics cards to solve faster algorithms with lower power consumption. When the graphics cards were operated with the factory default settings, none of them could profit from the current exchange rates. Reducing the power consumption along with increasing the speed of the algorithm has been an important factor in the transition to the profit zone. As a result of the studies, a performance increase of 30% is observed. Also, the electrical energy consumed by the graphics cards used for Ethereum mining is reduced by 20 to 30 percent.

Keywords: Ethereum, Blockchain, Cryptocurrency mining, GPU mining.

ETHEREUM MADENCİLİĞİNDE GPU PERFORMANSLARININ KARŞILAŞTIRILMASI VE İYİLEŞTİRİLMESİ

ÖZET

2008 yılında yayınlanan "Bitcoin: A Peer-to-Peer Electronic Cash System" adlı makale sayesinde bilgi sahibi olduğumuz Bitcoin, bilimsel litaratüre yeni terimler kazandırarak popülerliğini arttırmaktadır. Alternatif sanal para olarak geliştirilen Ethereum, merkezi bir sunucu veya bir kontrol noktaya ihtiyaç duymadan, karşılıklı uçlar arası anonim ve ucuz şekilde varlık transferine olanak sağlayan bir sistemdir. Blokzincir yapısının en yaygın kullanımı olan Bitcoin ve altcoinlerdir. Kripto paralar madencilik olarak adlandırılan ve zorlu bir algoritmanın çözümü ile gerçekleşmektedir. Sistemde yer alan herhangi bir madenci bu çözümü elde etmek için elinde bulunan ekran kartı ve işlemci gücünü kullanmaktadır. Bu çalışmada GPU'ların barındırdığı işlemcilerin, kayan noktalı işlem hesaplamalarında daha verimli olmaları sebebiyle Ethereum madenciliğinde kullanılan çeşitli ekran kartlarının performansları 4 kademeli bir iyileştirme paketi ile artırılarak karşılaştırılmıştır. Önerilen iyileştirme metotları için kullanılan ekran kartlarının model ve bellek miktarları şu şekildedir: 4 GB AMD R9 290, 4 GB AMD R9 380, 8 GB AMD R9 390, 4 GB AMD RX 560, 4 GB AMD RX 470, 4 GB AMD RX 480, 4 GB AMD RX 570, 4 GB AMD RX 580, 6 GB NVIDIA GTX1060, 8 GB NVIDIA GTX1070, 8 GB NVIDIA GTX1080. Bu çalışmanın en önemli amacı, Ethereum madenciliğine özgü Ethash özet algoritmasında iyileştirme yöntemleri uygulamaktır. Bu amaçla, AMD ve NVIDIA yonga seti grafik kartlarının daha düşük güç tüketimi ile daha hızlı algoritmalar çözmelerini sağlamak için iyileştirmeler yapılmıştır. Grafik kartları fabrika ayarlarıyla çalıştırıldığında, hiçbiri geçerli döviz kurlarından dolayı fayda getiremeyecek durumdadır. Algoritmanın hızını arttırmanın yanı sıra güç tüketimini azaltmak kar bölgesine geçiş için önemli bir faktör olmuştur. Yapılan çalışmalar sonucunda elde edilen değerlere bakıldığında yaklaşık % 30 performans artışı görülmüştür. Ayrıca iyileştirme paketi ile ekran kartlarının tükettiği elektrik enerjisi yüzde 20 ile yüzde 30 arası azaltılmıştır.

Anahtar Kelimeler: Ethereum, Blokzincir, Kripto para madenciliği, GPU madenciliği

CONTENTS

M.Sc. THESIS EXAMINATION RESULT FORM……ii

ETHICAL DECLARATION……...……iii

ACKNOWLEDGMENTS……...…...….iv

ABSTRACT…….….v

ÖZET……...…vi

NOMENCLATURE……ix

LIST OF TABLES……..…….....x

LIST OF FIGURES……..……..…. xi

CHAPTER 1 – INTRODUCTION……1

CHAPTER 2 – CRYPTO MONEY OVERVIEW…….……..6

2.1 Bitcoin…….6

2.2 Ethereum……...12

CHAPTER 3 – ALGORITHMS USED IN CRYPTO COINS.....16

3.1 Keys and Addresses……..16

3.2 The State of KECCAK-256 Hashing Algorithms……18

3.3 Hashing and Proof of Work…….……19

CHAPTER 4 – ETHEREUM MINING OPTIMIZATION TECHNIQUES…...22

4.1 Mining Architecture……..22

4.2 Ethereum Mining with AMD GPUs…….24

4.3 Ethereum Mining with NVIDIA GPUs…….25

4.4 Optimization Methods……...26

4.4.1 Power Limiting……...26

4.4.2 VRAM Timing Modification……..27

4.4.3 Undervolting and Core Underclocking……...29

4.4.4 VRAM Overclocking……..…30

4.5 Application of Optimizations for RX580 and GTX1080 Graphics Cards..30

4.5.1 Optimizations Application for AMD RX 580 4GB Graphics Card……31

4.5.2 Optimizations Application for NVIDIA GTX 1080 8GB Graphics Card…….34

CHAPTER – 5 CONCLUSION……...38

REFERENCES……...……...40

CURRICULUM VITAE……..….42

NOMENCLATURE

Acronyms

ASIC	Application Specific Integrated Circuit
ATM	Automatic Teller Machine
BIOS	Basic Input/Output System
DAO	Decentralized Autonomous Organizations
ECDSA	Elliptic Curve Digital Signature Algorithm
EVM	Ethereum Virtual Machine
GPU	Graphics Processing Unit
kWh	Kilowatt hour
Mh/s	Mega hashes per second, hash rate
mV	Millivolt
NIST	National Institute of Standards and
PoS	Proof of Stake
PoW	Proof of Work
RAM	Random Access Memory
ROM	Read-Only Memory
SHA	Secure Hashing Algorithm
SSD	Solid State Disk
TCP	Transmission Control Protocol

LIST OF TABLES

Table 4.1 Factory settings of AMD GPUs……..……25

Table 4.2 Factory settings of NVIDIA GPUs…….……25

Table 5.1 Results of measurement……..39

LIST OF FIGURES

Figure 2.1 Bitcoin price chart……..7
Figure 2.2 Bitcoin transaction life cycle…….....9
Figure 2.3 Blockchain data for Bitcoin……..10
Figure 2.4 Ethereum price chart…….13
Figure 2.5 Blockchain data for Ethereum…….....14
Figure 3.1 Digital signature……17
Figure 3.2 KECCAK256 sponge construct operations acting on an input……...19
Figure 3.3 Challenge response protocols scheme……..20
Figure 3.4 Solution verification protocol scheme……..21
Figure 4.1 Mining environment……..23
Figure 4.2 MSI Afterburner program interface…….…..27
Figure 4.3 GPU-Z GPU info tool……..…..28
Figure 4.4 Polaris BIOS editor for AMD graphics cards……..…...…28
Figure 4.5 Windows BIOS flashing Tool for AMD graphics cards……...29
Figure 4.6 OverDrivenTool for AMD graphics card voltage modifications……..….30
Figure 4.7 Hash rate of RX580 4GB graphics card without optimizations……..31
Figure 4.8 Profit calculation of RX580 graphics card without optimizations…….32
Figure 4.9 Hash rate of RX580 graphics card with optimizations…….....….33
Figure 4.10 Profit calculation of RX580 graphics card with optimizations……..34
Figure 4.11 Hash rate of GTX1080 graphics card without optimizations…….35
Figure 4.12 Profit calculation of GTX1080 graphics card without optimizations….36
Figure 4.13 Hash rate of GTX1080 graphics card with optimizations……..37
Figure 4.14 Profit calculation of GTX1080 graphics card without optimizations….37

CHAPTER 1

INTRODUCTION

Bitcoin can be defined as the sum of all technologies and concepts related to the virtual money ecosystem. The Bitcoin currency can be transmitted between all participants involved in the Bitcoin network. Bitcoin users can communicate with each other through the internet via the Bitcoin protocol. The Bitcoin protocol is open source and can be run directly on any device with a processor.

Users can transfer alternative crypto coins, such as Bitcoin or Ethereum, over the internet to do everything they can with conventional currencies, such as buying and selling goods and sending money to other users. Crypto money technologies include features based on encryption and digital signatures to secure the network. Crypto coins can be traded, sold and also converted to other cryptocurrencies [1].

Unlike conventional currencies, Bitcoin and alternative coins are completely virtual and based on blockchain technology. In money, a virtual unit, which is defined as value only, is sent from the sender to the recipient. Crypto money users can prove that they own the cryptographic key with their cryptographic key and spend the crypto money they earn from the transaction or transfer it to a new buyer. These keys are usually saved in a digital wallet on each user's computer. Having the key that unlocks a transaction is the only condition for spending the money available so that the control by the system is completely left to the user's hands.

Although it is generally associated with Bitcoin, Blockchain technology has many other applications that go beyond digital currencies. Bitcoin is just one of several hundred applications that use Blockchain technology today. Until relatively recently, blockchain applications required a complex background in coding, cryptography, mathematics, and key resources. From electronic voting to digitally recorded real estate assets and trade, applications that have never been used before are now actively being developed and used [2]. Ethereum, which provides developers with tools to create decentralized applications, makes all this possible [3].

In its simplest form, Ethereum is an open source software platform based on Blockchain technology that enables developers to create and deploy decentralized applications. Like Bitcoin, Ethereum is also a public network. Although there are some important technical differences between the two, the most important distinction to be noted is that Bitcoin and Ethereum differ significantly in purpose and ability. Bitcoin offers a unique Blockchain technology application for a peer electronic cash system that allows online Bitcoin payments [1]. While Bitcoin is used to monitor Blockchain technology for the ownership of digital money, Ethereum focuses on running Blockchain technology with the programming code of any decentralized application [3]. In the Ethereum blockchain, instead of mining for Bitcoin, the miners try to win Ether, a crypto-money that feeds the network. Beyond a useful cryptocurrency, Ether is also used by application developers to pay for fees and services on the Ethereum network [3]. There is a second type of block used to pay the miners' wages and it is called gas. Each smart contract application requires a certain amount of gas to be sent to convince miners to place them in the blockchain.

A smart contract is an expression used to describe computer code that will facilitate the exchange of money, content, property, shares, or any value. An intelligent contract running on Blockchain is like a self-running computer program when certain conditions are met. Because smart contracts work in the blockchain, they operate fully programmed without censorship, hitch, forgery or third-party interventions. All blockchains are capable of code processing, while most are severely limited. Ethereum is different. Instead of providing a few limited operations, Ethereum enables developers to do whatever they want. This means that developers can create thousands of different applications that go beyond anything it's seen before [3].

Before the creation of Ethereum, very limited Blockchain applications were designed to perform a series of operations. For example, Bitcoin and other cryptocurrencies have been developed to work only as peer-to-peer digital currencies. Developers faced a problem. Developers had to expand the set of functions offered by Bitcoin and other very complex, time-consuming types of applications, or create a new Blockchain application and a completely new platform. The creator of Ethereum, Vitalik Buterin, adopted a new approach. Ethereum Virtual Machine (EVM), the core innovation of

Ethereum, is a Turing software running on the Ethereum network. Enables the execution of any program regardless of the time and programming language required. Ethereum Virtual Machine makes the process of creating Blockchain applications easier and more efficient than ever before. Instead of building a completely original Blockchain for every new application, Ethereum allows thousands of different applications to be developed on a single platform [3].

Ethereum is a project that tries to build generalized technology which all process-based state machine concepts can be built on. This big project has many goals. One of these is to facilitate and accelerate the transactions between the individuals who cannot trust each other. The basis of this insecurity may be due to geographical separation, the difficulty of confrontation or the non-compliance of existing legal systems. Agreements in this proposed system will have various features that are not common in the real world. Vitalik Buterin first proposed the core of this study in late November 2013. Although it developed in many ways by 2019, the basic functionality of a blockchain with effective in-process storage capability remained unchanged [4].

Ethereum allows developers to create and deploy decentralized applications. A decentralized application serves a specific purpose for its users. For example, Bitcoin is a decentralized application that provides a peer-to-peer electronic cash system that allows users to pay online Bitcoin. Since decentralized applications consist of code running on a Blockchain network, they cannot be controlled by any individual or central entity. Centralized services can be deployed using Ethereum. Imagine all the brokerage services that exist in hundreds of different industries. For example, obvious services such as loans to brokerage services by banks, voting systems. Ethereum can also be used to create Decentralized Autonomous Organizations (DAO) [5]. Since decentralized applications work on the blockchain, they benefit from all the features of the blockchain.

Invariance: A third party cannot make any changes to the data.

Evidence of Bribery and Bribery: Applications are based on a network built around the principle of censorship, making censorship impossible.

Security: Applications are well protected against attack attacks and fraudulent activities without a central point of failure and secured using cryptography.

Zero Failure: Applications never become unusable and can never be turned off.

Although there are many benefits, decentralized applications are not perfect. The smart contract code is written by people, smart contracts are just as good as the people who write them. Code errors or oversight may cause undesirable negative behavior. If an error in the code is exploited, there is no effective way to stop an attack or exploitation except to obtain a network consensus and rewrite the underlying code. This is against the nature of the blockchain intended to be invariant. In addition, any action taken by a central party may raise serious questions about the decentralized nature of an application.

Ethereum, unlike other crypto algorithms GPUs can be used to mine the Ethash algorithm which is the algorithm of Ethereum. So, if you want to do mining firstly, you need to use the graphics cards. On the one hand, when you think about an ASIC device and the ASIC chips one by one when you watch the deterioration of the chips do not come. But you can benefit from the "Guarantee" process when your graphics card is broken. On the other hand, because GPU technology is not like ASIC technology, there is no difficulty in logarithmic increases. In other words, if there is a graphics card in the market, there is a difficulty in increasing the number of cards with linear proportions, while the other coins mining with ASIC device is progressing logarithmically [6].

The case described as the difficulty of the case of a certain production planning crypto money in that year to balance the excess production of the power of the mining power to survive compared to the state of the decline. In other words, 1 Ethereum can be excavated with 200 Mh/s in a month and 200 Mh/s and 0.90 Ethereum can be excavated with difficulty increase. The graphics cards used in Ethereum mining provide a mining speed according to the hardware power they use when used in factory configuration. Up to 6 graphics cards connected to a computer can be connected to the network and started mining through the program. In doing so, of course, power is consumed in the order of kWh. In order to obtain profit from Ethereum mining,

parameters such as mining speed and electrical expense should be calculated and followed. Using various improvement techniques, graphics cards can be used to speed up mining and consume less electricity. In this thesis, it is shown that it is possible to make more profit from Ethereum mining by applying a 4-stage improvement package.

Within the scope of the thesis, techniques will be presented to facilitate Ethereum mining excavated by process power owners all over the world and to reduce energy consumption and make them more efficient. The performance of 11 different chipset graphics cards, AMD and NVIDIA, will be measured, compared and compared with other technical solutions. Improvement in AMD chipset graphics cards has been influential in both power consumption and mining speed. The same mining speed on the NVIDIA chipset graphics cards will be achieved with lower power consumption. In this way, the energy consumption of mining operations will be reduced. In Chapter 2, detailed information about Bitcoin and Ethereum will be given, in particular, what kind of operations a user on the network has in the system and the life cycle of these processes will be explained. Section 3 cryptographic substructure of the Ethereum will be detailed. Chapter 4 will describe the 4-step speed and electrical energy modifications and its applications for RX580 4GB and GTX1080 8GB will be given. In the last part, the results will be examined.

CHAPTER 2

CRYPTO MONEY OVERVIEW

Crypto money is a currency system such as Turkish Lira and Dollar. But unlike these currencies, the purpose of creating crypto money is to provide digital information exchange with a process that is made possible by certain cryptography principles. The purpose of cryptography is to secure money transactions and control the creation of new funds. The first Crypto money was Bitcoin in 2009. Today, hundreds of different cryptocurrencies are used and they are often called "alternative crypto money. Nowadays the most famous crypto money is Bitcoin and Ethereum in 2019.

2.1 Bitcoin

Bitcoin is a virtual currency that is universal and decentralized not connected to any state or other legal entities [7]. Satoshi Nakamoto has created an electronic money system which has not been completely centralized by combining some previous similar applications like b-para and HashCash and published his work in 2008 with an article titled Bitcoin: A Peer to Peer Electronic Cash Payment System. In this work, Bitcoin claims that it is a fully point-to-point electronic currency with no need for any organization or third party [7]. The electronic payment system designed according to the proposal is based on cryptographic evidence rather than the trust mechanism in the old methods. As a result of this approach, when the two parties make purchases with each other, no third party is needed to verify this exchange. The proposed system is as follows. When the money is exchanged, each user sends the money to the next one and signs his own with the digital signature, the previous transaction summary, and the next owner's public key. The receiving party can confirm this signature with the public key of the sending party to determine whether the transaction belongs to it.

The key innovation in the Bitcoin system is in the solution of the double spending problem, which is the most important weakness of the previous digital currencies. The problem is that the payment area cannot verify that one of the previous owners in the

chain has not used the money twice. A common solution is that a central authority (bank, center) checks whether each operation is a duplicate operation. After each transaction, the money returns to the center and a new currency is put in place. It can be assured that the money put on the market directly by the center has not been spent twice. The problem in this solution is that the whole system of the monetary system is in the hands of a central organization, such as the bank, where each transaction goes through. There is a need for a method by which the recipient can verify that the previous owners of the money have not signed the transaction in advance. The only way to prove that an action has not occurred is to be informed of all transactions. To be able to do this without a trusted party, transactions must be publicly announced. In this, Nakamoto's suggestion is as follows; In the Bitcoin system, all money transfers are collected on a ledger which shows how much money is gone, when, and how much money, and in this account, the amount of money in the account is kept and the same money is wasted.

Satoshi Nakamoto's invention is a practical solution to a problem previously unresolved in the distributed calculation, known as the Byzantine Generals problem [1]. In short, the solution of Satoshi Nakamoto, who uses the Concept of Business Proof to ensure consensus without a reliable central institution, is thought to be a breakthrough in the sciences of distributed systems and has wide applicability beyond the currency. It can be used to provide compromise on decentralized networks for demonstrable fair elections, lotteries, asset records, digital notary certifications, and more.



Figure 2.1: Bitcoin price chart [8].

The Bitcoin network was launched in 2009, based on a reference application published by Nakamoto and revised by many other programmers. Distributed computing, which provides security and flexibility for Bitcoin, has increased exponentially and is now surpassing the processing capacity of the world's largest supercomputers [1]. As shown in Figure 2.1 total market value of Bitcoin is estimated to be between 10 billion USD and 20 billion USD, depending on the USD/Bitcoin exchange rate. Until now, the largest transaction processed by the system was 150 million USD and was processed at no cost.

Bitcoin is a fully distributed, peer-to-peer system, but cryptographic techniques have been applied to ensure integrity and anonymity. Therefore, there is no central server or control point. Bitcoins are formed by a process called mining that looks for a solution to a difficult problem. Any participant in the Bitcoin network (i.e. any device that uses the Bitcoin protocol stack) can work as miners using the computing power of their computers to try to find a solution to this problem. On average, every 10 minutes a user in the Bitcoin network has a new solution that verifies the validity of the last 10 minutes of transactions and is rewarded with new Bitcoins. Basically, Bitcoin mining decentralizes the money-making and distribution of a central bank and eliminates the need for any central bank.

It can be explained what steps a new user should join to the Bitcoin network. First, it must install its virtual wallet on its computer or mobile device to store its Bitcoins. After performing this operation, it must have its own address value, the public key that is accessible to everyone and the private key which belongs to itself. After completing this process, the virtual currency required to perform a purchase with Bitcoin can be provided in four ways. The most common of these is the acquisition of Bitcoin from a friend or a friend who uses Bitcoin, the purchase of Bitcoin ATMs based on exchange/Bitcoin exchange, the sale of a product or service for Bitcoin and accessing Bitcoin sellers via some websites. When a new user in Bitcoin wants to purchase with Bitcoin after having done the above transactions, it can be summarized the chain of transactions occurring in the system as follows in Figure 2.2. Firstly, the product or service opens the virtual wallet on the person's computer or mobile device, and by

scanning the frame code containing the address of the person who owns the service and the product, he/she can easily access the related person's information.

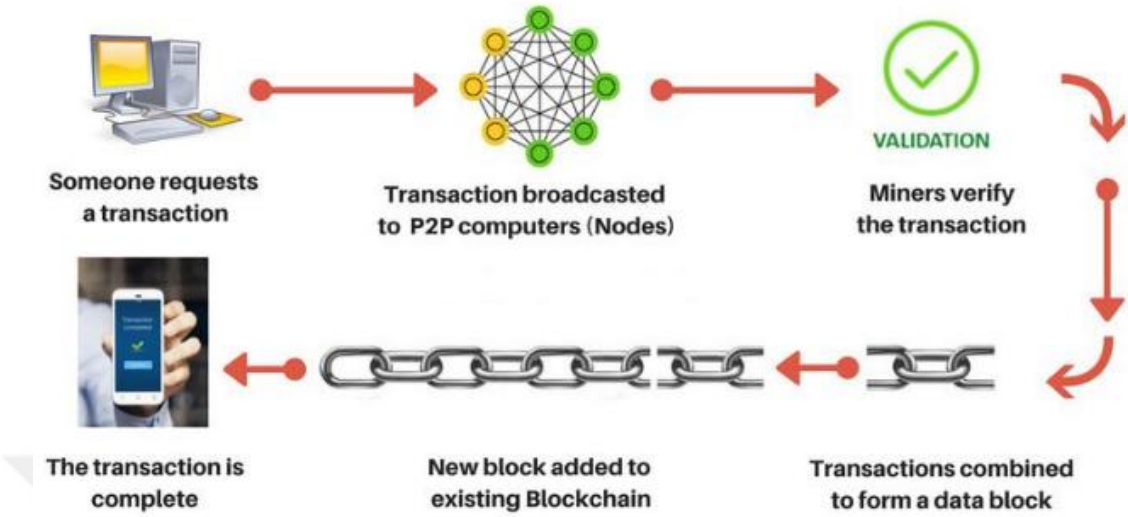
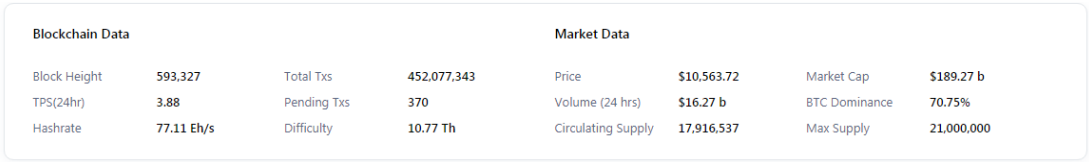


Figure 2.2: Bitcoin transaction life cycle [9].

It completes the virtual money transfer process by adding the amount to be paid to the person to whom the information reaches and the transaction fee to be given to the Bitcoin mining operator. The user will now finish the process, and the subsequent operations will be done by the Bitcoin system and by the Bitcoin miners. In addition to the amount of virtual money sent at this stage, the digital signature is created by the wallet with the help of the person's private key and this information is published and approved by all users in the Bitcoin network. In order to gain the new Bitcoin prize, the miners in the Bitcoin network will be included in the transaction set called block. After that, miners run SHA256 summary algorithms in their hardware to solve the problem of business. Once a miner has solved the proof of a business problem, he publishes the new block in the Bitcoin network. Block is verified by the nodes in the network, the miner producing this block is now rewarded with 12.5 BTC, and the summary value of the previous block is used when creating a new block so that the nodes accept the block. When a new block is generated after the accepted block, the person who receives the Bitcoin as a result of the exchange now understands that the transaction is valid and sends the product or service that needs to respond to the virtual money to the buyer. Electronic cash payment system the operating principles of Bitcoin are briefly carried out in this way and the same life cycle is repeated for each process.



Blockchain Data				Market Data			
Block Height	593,327	Total Txs	452,077,343	Price	$10,563.72	Market Cap	$189.27 b
TPS(24hr)	3.88	Pending Txs	370	Volume (24 hrs)	$16.27 b	BTC Dominance	70.75%
Hashrate	77.11 Eh/s	Difficulty	10.77 Th	Circulating Supply	17,916,537	Max Supply	21,000,000

Figure 2.3: Blockchain data for Bitcoin [10].

Figure 2.3 shows the blockchain data for Bitcoin. Here it can be seen that the difficulty level is considerably higher than the Ethereum difficulty level shown following section. The terms that are important in the Bitcoin system are described below.

Block: It is a structure that does not take place in previous blocks or contains some Bitcoin operations. New blocks are produced by Bitcoin mining and are added to the blockchain formed by previously accepted blocks. The block with which the transactions are located is included in the blockchain when it is verified by a person. The blockchain solves the problem of using more than one Bitcoin. In the meantime, the most important part of the block is very important for Bitcoin mining. Each block comprises a summary of the cap portion of the block which was produced before it, thereby providing the formation of a chain structure.

Process: The Bitcoin process can be called a Bitcoin transfer between the receiver and the sender. Communication must be secure to avoid fraud, such as counterfeiting. To ensure secure communication, documents created by an organization such as transcripts can be digitally signed. The digital signature uses a number of encryption policies. Each transaction is collected in blocks and digitally signed from point-to-point in the Bitcoin network before being broadcast. Bitcoin is traded during the transaction and the security of this process is based on the Elliptic Curve Digital Signature Algorithm (ECDSA) [11,12]. The buyer wishes to make sure that Bitcoin is not used more than once, and as described above, a list of all transactions is provided to all points.

Proof of Work and Longest Chain: Proof of a job is a piece of data that is difficult to achieve in terms of time and cost. The data obtained must be controllable in a very simple way. The production of proof of business can be a very low probability random process, thus requiring many trials and errors on average to achieve the goal. In

Bitcoin, the Proof of Work (PoW) was carried out to increase the nonce area in the block header until the block header summary value contained a certain number of zeros in the initial part.

The PoW is used to create blocks. PoW attached to the data of each block is required for the acceptance of this block by the network. The challenge is set to allow the Bitcoin network to create a block in approximately 10 minutes. Since the probability of creating a successful block is very low, it is unpredictable which miners in the network will work on the next block.

For a block to be considered valid, the block summary must be smaller than the target value. If such a block summary value is found, it is understood that the work proof problem has been solved and a certain amount of workload has been made. Each block contains a summary of the block before it so that each block contains a blockchain and a high workload together. It is possible to change a block (but it is possible by creating a new block containing the previous block) by rebuilding all the blocks that come after it and by repeating the entire workload that they contain. With this method, the blockchain is protected in such a way that it cannot be played on [7].

Target: This value is a 256-bit integer shared and published by the Bitcoin community. This value determines the difficulty of finding the solution to the work proof problem in Bitcoin. A basic requirement by the Bitcoin protocol for the acceptance of a block; the summary value of the block header is defined as being smaller than the current target value. Therefore, the reduction of the target value means that the creation of a new block with Bitcoin mining is becoming more difficult. The target value is assigned a new value after the last 2016 block has been removed. Each block is removed approximately every 10 minutes so that the 2016 block takes approximately 2 weeks. As a result, the change in the target value after two weeks is made difficult to prove the problem of work.

2.2 Ethereum

Ethereum runs programs called smart contracts which called ether and it is an open source, globally decentralized computing infrastructure. To block and store system state changes, a blockchain uses an encryption currency, called ether, to limit execution resource costs [3].

The developers develop applications by using the Ethereum platform that has a variety of economic functions, away from centrality. Reduces various counterparty risks while delivering high availability, auditability, transparency, and impartiality.

Ethereum was designed at a time when people began financial transactions using the power of the Bitcoin model and tried to develop other applications using crypto applications. But developers had to make a choice. The first one was Ethereum's construction of Bitcoin. The second was the launch of a new blockchain. Building on Bitcoin could be interpreted as accepting the limitations of this system and overcoming problems with some solutions. Limited transaction types, data types, and data storage sizes seemed to limit the range of applications that could run directly in Bitcoin. This eliminated some of the advantages of using a public blockchain. The only option for projects requiring freedom and originality while staying in the blockchain was a new blockchain structure. However, developing this new blockchain structure meant much more workload.

In December 2013, Vitalik Buterin wrote an article on the idea behind a general-purpose blockchain. Many developers have read this article and provided feedback to help improve the new system that Vitalik Buterin is considering [14].

Ethereum has different development architecture than Bitcoin. In Bitcoin, development is determined by much more stringent principles, and all changes are examined with great importance in order not to spoil the existing structure. Most of the time, changes are only applied if they are retrospectively compliant and are believed not to cause problems. Units in the current system are allowed to register, but if the units do not upgrade, the system will continue to run in the same way.

In Ethereum, the continuation of the structure is shaped depending on the future, not the past. If a change needs to be made, this is applied even if it means overriding previous system parameters, disrupting compatibility, or forcing users to update. Ethereum's development steps can be defined as a rapid innovation, rapid evolution, and a tendency to implement improvements for future reference, even at the expense of some backward compatibility. For an Ethereum application developer, this means that you must stay flexible and be willing to rebuild your infrastructure from the beginning as the underlying structure becomes new. One of the biggest problems faced by application developers in Ethereum is the contradiction between deploying the developed code into a system that cannot be changed and an ever-evolving infrastructure. You cannot only upgrade your smart contracts and be prepared to deploy new contracts and migrate customers and software to the new system. This also means that platforms with more flexibility, independence, and less central control are still not achievable at the desired rate. Independence and local government require a little more stability than the possibility of entering Ethereum in the next few years. You must be ready to restart your smart contracts to develop the platform. This means that you need to have an effective control mechanism over your smart contracts [3].

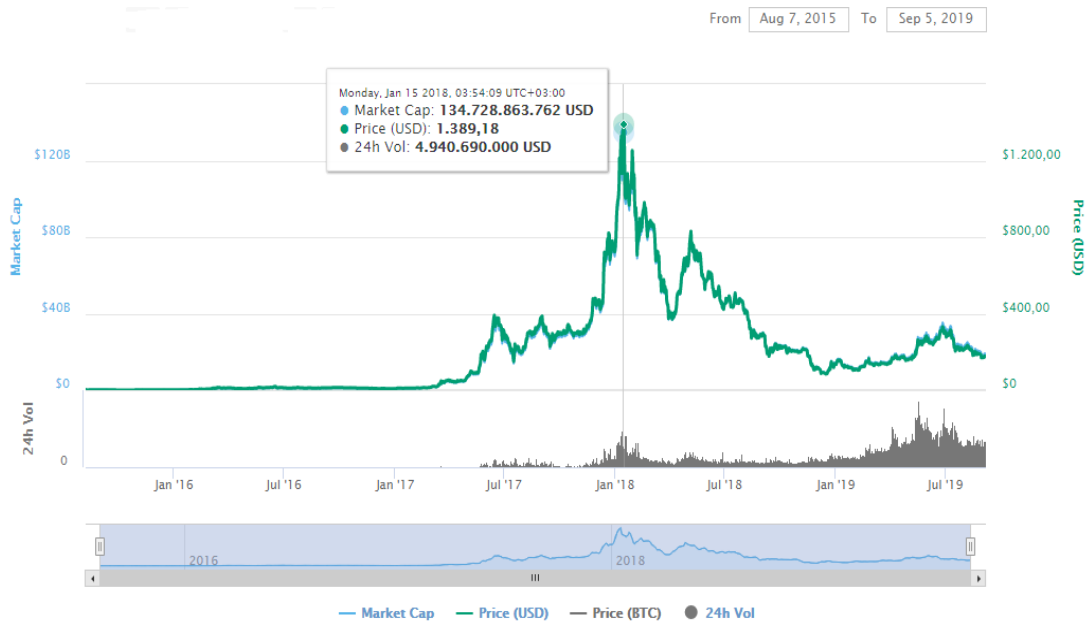


Figure 2.4: Ethereum price chart [13].

As shown in Figure 2.4 total market value of Ethereum is estimated to be between 140 USD and 1200 USD, depending on the USD//Bitcoin exchange rate. Until now, the largest transaction processed by the system was about 1400 USD and was processed at no cost.

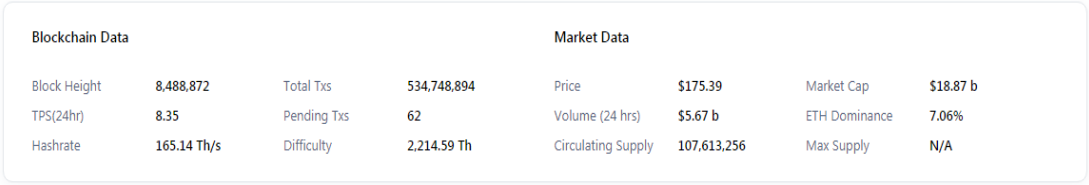


Figure 2.5: Blockchain data for Ethereum [15].

Figure 2.5 shows the blockchain data for the Ethereum. The block length, hash rate, and difficulty level are displayed here. The terms that are important in the Ethereum system are described below.

Difficulty: Difficulty is one of the basic parameters of Bitcoin, Ethereum and all other mineable cryptocurrencies. It is a parameter that crypto money networks use to keep the average time between blocks constant as the hash rate parameter changes.

P2P Network: Ethereum operates on the main Ethereum network, which can be addressed on TCP port 30303.

Consensus Rules: Ethereum's basic development rules are published in the reference declaration.

Transactions: Ethereum operations are small network-based messages that include the sender, the recipient, the value, and the data load.

State Machine: Ethereum state transitions are handled by the Ethereum virtual machine, a virtual machine that executes byte code. These virtual machine programs, called smart contracts, are written in high-level programming languages and compiled into byte code to execute on the Ethereum virtual machine.

Data Structures: The current state of Ethereum is stored locally in a database file on each node. It stores processes and system states in a serialized mixed data structure called a Merkle Patricia Tree.

Consensus Algorithm: Ethereum has adopted the Nakamoto Consensus, the infrastructure model of Bitcoin's infrastructure, and uses sequential single signature blocks. These blocks are important for determining the longest chain and therefore the current situation by PoW. However, plans to switch to a PoS-based system called Casper in the near future are being discussed.

Economic Security: Ethereum is currently processing a PoW algorithm called Ethash. However, it is unclear how long this situation will continue. It is planned to switch to the PoS system.

CHAPTER 3
ALGORITHMS USED IN CRYPTO COINS

One of the major disciplines used by Ethereum is cryptography, the mathematics that is used frequently in computer security. Encryption is used to store the content of the information to be stored and to make it clear again when necessary [16]. Such encryption evidence is the mathematical tools necessary for the operation of Ethereum technology and all blockchain systems. In addition, these codes are widely used in Ethereum applications. To ensure secure communication, documents created by an organization such as transcripts can be digitally signed. The digital signature uses a number of encryption policies. The cryptographic summary functions serve as a basic building block to ensure information security. Cryptographic summary functions do not provide complete information security on their own, but they are critical to information security programs. Therefore, in information security projects, cryptographic summary functions significantly affect the overall security and computational efficiency. The cryptographic summary function is a process that converts input data of any length into a fixed length output [3].

3.1 Keys and Addresses

A key to decrypt and which may be different for each password consists of only a randomly assigned number [17]. The owner of the private key is the owner of the key to access to contracts authorizing this address, as well as user control over all funds associated with the Ethereum address [18]. The private key is used to generate the signatures required to spend Ethereum by proving ownership of the funds used in a transaction. This key needs to remain confidential because explaining this to the other parties is the same as transferring control over Ethereum and other assets owned. This switch must be backed up by various backup mechanisms. If the key is lost, the assets

are now completely lost. Public key encryption is now the main part of the information security sector [19].

Public key encryption protects information with dissimilar key elements. These switches are based on mathematical functions with unique properties. These functions enable the creation of digital secrets and difficult digital signatures, secured by encryption and mathematical laws. Private keys do not function directly in the Ethereum network and are not stored. Only account addresses and digital signatures that have been used so far are transmitted and stored in the system as part of the Ethereum network.

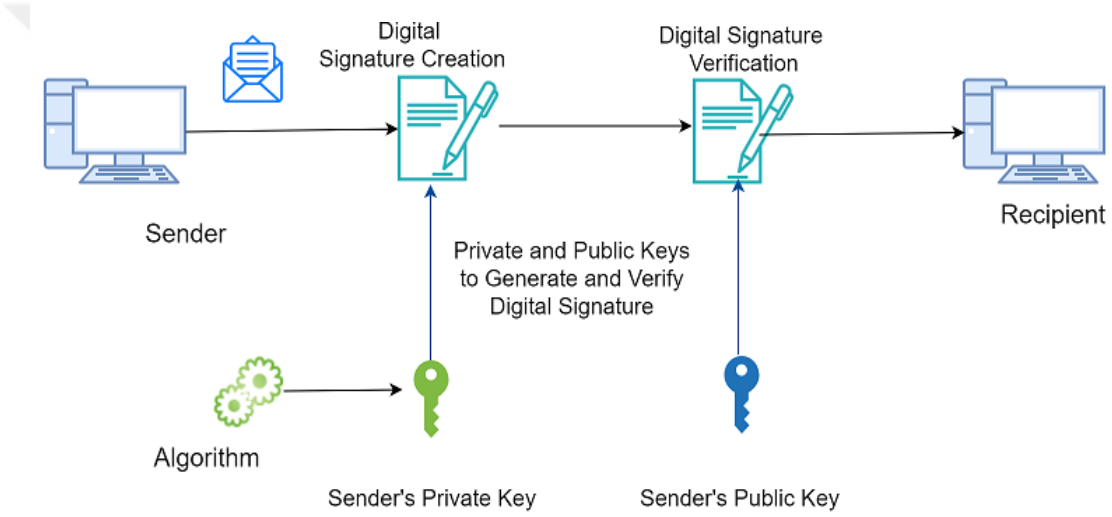


Figure 3.1: Digital signature [20].

Mathematical functions implemented using an elliptical curve form an advanced category of functions in terms of cryptography. Arithmetic operations can be performed easily in elliptic curve systems, but reversing is impossible. This is called a discrete logarithm problem and there is still no possibility [21]. Using elliptical curves, cryptography is often used in today's advanced computer systems and is the basis for Ethereum use of private keys and digital signatures [22].

Ethereum addresses are descriptors generated from keys generated using the Keccak-256 algorithm. Ethereum uses many Keccak-256 encryption hash functions. In 2006 National Institute of Science and Technology (NIST) from the US organized a

competition about Cryptographic Hash Functions. Keccak-256 was one of the candidates [23]. Result of the competition Keccak algorithm won and in 2015 Federal Information Processing Standard agreed on this algorithm as one of the standard cryptographic Hash algorithms. Ethereum addresses are hexadecimal numbers and are derived from the last 20 bytes of the Keccak-256 hash.

3.2 The State of KECCAK-256 Hashing Algorithms

SHA-3 serves as a random source for the inputs to the hashing algorithm, while it exhibits some variation in itself with a mechanism known as a sponge structure that uses random permutations to reveal the data. In the example below, a public key was derived by using elliptic curve multiplications.

Private key k:

k =

f8f8a2f43c8376ccb0871305060d7b27b0554d2cc72bccf41b2705608452f315 (3.1)

Public key K (x and y coordinates concatenated and shown as hex):

K =
6e145ccef1033dea239875dd00dfb4fee6e3348b84985c92f103444683bae07b83b5c38e5e... (3.2)

Keccak-256 to calculate the hash of this public key:

Keccak256(K) =
2a5bc342ed616b5ba5732269001d3f1ef827552ae1114027bd3ecf1f086ba0f9 (3.3)

Then keep only the last 20 bytes (least significant bytes), which is our Ethereum address:

001d3f1ef827552ae1114027bd3ecf1f086ba0f9 (3.4)

Most often see Ethereum addresses with the prefix 0x that indicates they are hexadecimal-encoded, like this:

0x001d3f1ef827552ae1114027bd3ecf1f086ba0f9 (3.5)

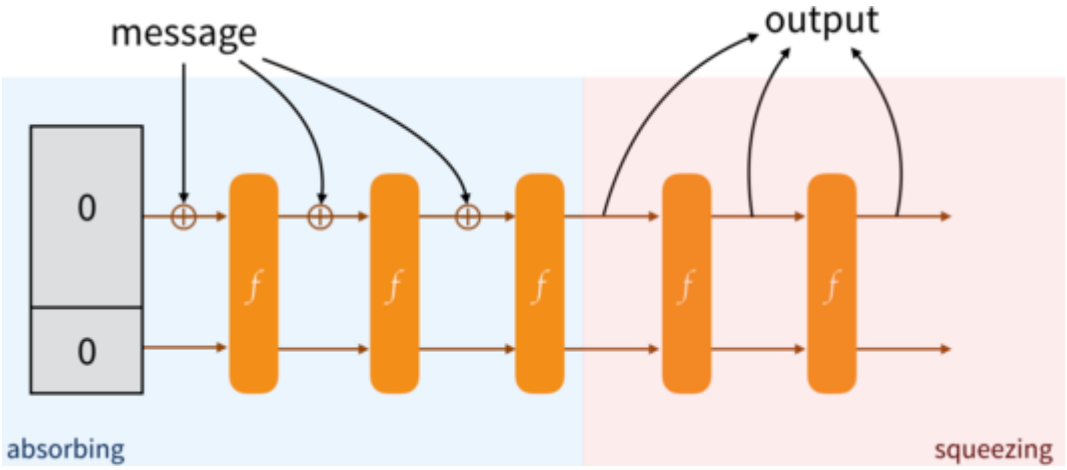


Figure 3.2: KECCAK256 sponge construct operations acting on an input [24].

Absorbing The original message M is subjected to mnogoraundovaya the permutation f. Squeezing (pressing). The output of the resulting permutations of the value z.

3.3 Hashing and Proof of Work

Bitcoin chose SHA256 as a hash algorithm, and Ethereum chose SHA3, Keccak-256, for proof of the operating system. Bitcoin is the oldest and Ethereum creators did not choose the algorithm as Bitcoin.

However, selecting a hash function for a blockchain using Business Proof is the activity of calculating that hash. Bitcoin SHA256 calculations can be performed efficiently by special circuits, which are Application-Specific Integrated Circuits. In other words, Proof of Work (PoW) encourages computationally efficient machine groups to accumulate in pools and measure what we call "mixed power or the number of hashes that a machine can calculate per time interval.

Ethereum, chosen as the PoW algorithm, is a modified SHA3 algorithm known as Keccak-256. Additionally, the PoW algorithm is memory sensitive to calculate calculations. Dagger-Hashimoto is the first version of the Ethereum algorithm. It uses the PoW system and was designed by Ethereum creator Vitalik Buter. The Ethereum team initially combined the critical features of the Hashimoto and Dagger algorithms. This is called the Dagger-Hashimoto algorithm and is a memory-intensive algorithm designed to withstand specific circuits integrated into the application. The Dagger-

Hashimoto and Ethash algorithms were then separated. However, both are still known as synonyms [26].

The PoW system is a consensus mechanism that allows preventing denial-of-service attacks. This attack, if that occurs, needs a job from a service request, often requiring computer action and other service violations such as spam on the network. Cynthia Dwork and Moni Naor presented this concept in 1993 with a paper. Markus Jakobsson and Ari Juels have formalized the concepts as written [25]. A key feature of this system is its asymmetry. It is very difficult on the demanding side of the work, but the service provider should be easy to control. This idea is also known as a CPU cost function, customer puzzle, computational puzzle or CPU pricing function. There are two working proof protocol classes.

Challenge response protocols take on a direct interactive connection between the requester and the provider. The provider selects a challenge, tells an item in the set with properties, the requestor finds the corresponding response in the set, and is sent back and checked by the provider. Since the difficulty is chosen by the provider in situ, the difficulty can be adapted to the current load. Work on the requested side may be limited if the challenge response protocol is known to have a known solution or is located within a restricted search area as follows in Figure 3.3.

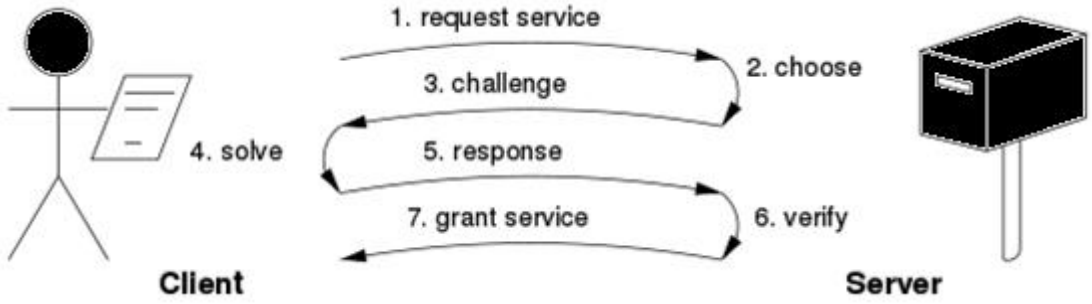


Figure 3.3: Challenge response protocols scheme [26].

The solution validation protocols do not have such a connection: as a result, the problem must be addressed automatically before a solution is sought by the claimant and the provider must control both the problem selection and the solution found as follows in Figure 3.4.

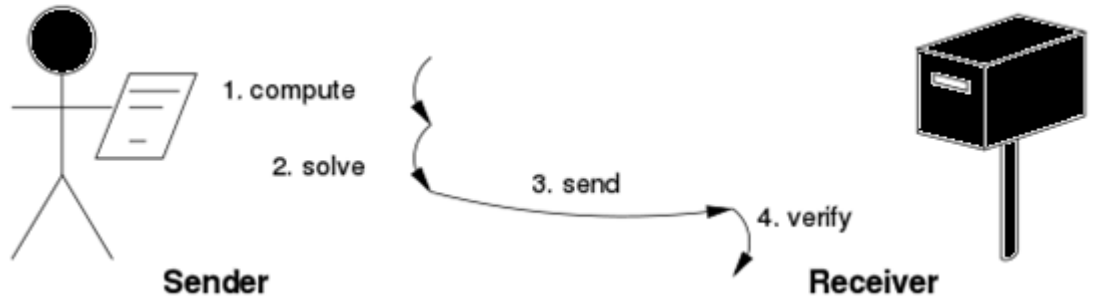


Figure 3.4: Solution verification protocol scheme [26].

CHAPTER 4

ETHEREUM MINING OPTIMIZATION TECHNIQUES

Ethereum mining could be done in the early years with graphics cards or processors. However, due to time and increasing difficulty, Ethereum mining can no longer be done efficiently and profitably. Ethereum mining is made possible by the systems that can solve the algorithm called Ethash. Today, Ethereum mining can be done with graphics cards using integrated circuits produced by AMD or NVIDIA companies. For the centralized feature required for the crypto money system to function, a large number of miners working on GPUs with the Ethereum algorithm is vital to the operation and safety of the system. Of course, it is very important for the professionals of this subject to make sure that the electrical energy and crypto coins are calculated and the profit or loss account is made. In this chapter, Ethereum mining architecture and the basic features of AMD and NVIDIA graphics cards used in the thesis will be given.

4.1 Mining Architecture

A large number of miners from all over the world continue to solve Ethereum, guaranteeing that the network can transfer assets much more reliably, quickly and smoothly. There are many open or closed source programs in Ethereum mining. In this study, the Claymore Dual Miner program was used because it supports both AMD and NVIDIA chipsets. However, the program runs on Windows 10 operating system for easy operation and compatibility. Other versions of Windows, especially multi-GPU systems, are insufficient in mining. Windows 10 is capable of combining 12 graphics cards in one system and defining them; Windows 8.1 and Windows 7 can run 4 graphics cards without any problem. For this reason, the operating system preference is used in the direction of Windows 10. MSI Afterburner 4.6 software is used to change and monitor the display features such as power limit, processor speed, memory speed,

fan speed, and processor voltage. The systems used in Ethereum mining are composed of basic computer parts. A processor, a motherboard with the required PCI-Ex slot, at least 4 GB of RAM, at least 700 Watts of power, and if possible gold-certified 80+ efficient power supply, at least 90 GB SSD, the riser card to bring the PCI-Ex slots to the appropriate position and to control the system, the monitor, keyboard, and mouse are the necessary hardware. The processor can be selected from Intel or AMD companies at current low-speed processors. In crypto-money mining made with graphics cards, the processing power does not affect the mining speed. In this study, the Intel G4400 processor with 3.3 GHz operating frequency is used. Minimal 4 GB of RAM is required for the Windows 10 operating system to work easily with the miner software. For both speed and temperature, SSD should be used as a hard disk in the system. The power supply is the most critical part of mining systems. Since the display cards will operate continuously, a power supply with a capacity to power at least 1.5 times the power consumption should be preferred. In this way, the power supply will be more efficient, which is an important parameter in terms of cost reduction. In Figure 4.1 mining environment is shown.

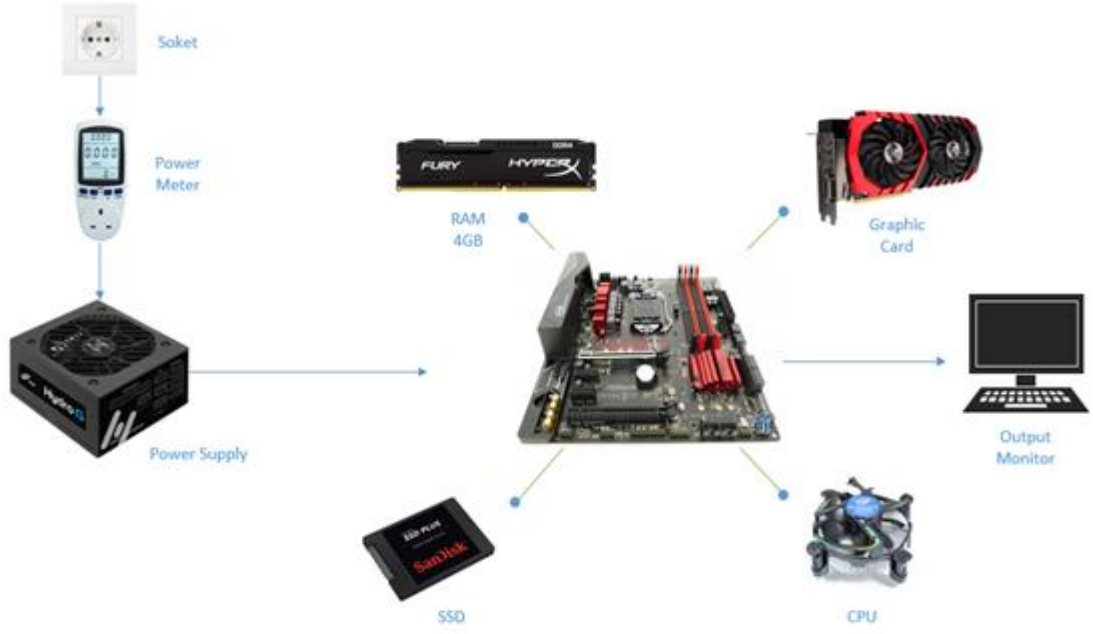


Figure 4.1: Mining environment

The EVGA 750 Watt Gold certified 80+ efficient power supply provides the required features. The difference between the power drawn from the socket and the used power

is low in terms of the profitability of the system in our country where the electricity is approximately 0.1 USD/kWh. A power meter plug was used to make the measurements. Below is given a list of devices that are used in the mining environment.

Motherboard: The motherboard has a B250 Intel chipset, 4x DDR4-2400/2133 DIMM slots and maximum capacity 64GB, 2x PCI-Express 3.0 x16 Slots (one runs at x4), 2x PCI-Express 3.0 x1 slots, multi-graphics which are supports AMD Quad CrossFireX, CrossFireX technology. Ports are 6x USB 3.0 ports, 6x USB 2.0 ports, 1x PS/2 mouse port, 1x PS/2 keyboard port, 1x VGA Port, 1x DVI-D Port, 1x HDMI Port, 1x RJ45 LAN Port, Audio I/O jacks.

PSU: The power supply unity has 700W and %88 power efficiency.

RAM: The random access memory is HyperX Kingston technology fury 2400MHz DDR4. It has easy to install plug-and-play functionality. Its operating temperature from 0° C to +85° C and storage temperature from -55° C to +100° C. It has automatic overclocking property to reach faster speeds and higher capacities just by installing the memory, no adjustments in BIOS needed. And also it is cost-efficient, the perfect combination of price and DDR4 performance.

SSD: The solid-state disk is SanDisk SSD PLUS 120GB Internal SSD - SATA III. It is an easy upgrade for faster boot-up, shutdown, application load and response. It boosts burst write performance, making it ideal for typical PC workloads. It has the perfect balance of performance and reliability. It has read/write speeds of up to 530MB/s/400MB/s. (Based on internal testing; performance may vary depending upon drive capacity, host device, OS and application.) It has shock resistant for proven durability even if you drop your computer.

CPU: The central process unit is Intel CPU BX80662G4400 Pentium G4400 3.30Ghz. It has socket LGA 1151 and Intel HD Graphics 610.

4.2 Ethereum Mining with AMD GPUs

Ethereum mining can be made with AMD chipset graphics cards. The fact that AMD brand cards can be further improved compared to NVIDIA chipset graphics cards is

an issue that miners have shown a lot of interest in. However, it should be noted that some more stability of AMD graphics cards is also a matter of concern. Graphics cards to be tested will be R9 290, R9 380, R9 390, RX 470, RX 480, RX 560, RX 570, RX 580.

Table 4.1: Factory settings of AMD GPUs

	R9 290	R9 380	R9 390	RX 470	RX 480	RX 560	RX 570	RX 580
GPU Core (MHz)	1000	990	1010	1242	1300	1300	1268	1411
GPU RAM (MHz)	5200	5500	6000	6600	7000	7000	7000	7000
GPU Supply (mV)	1300	1200	1300	1150	1200	1000	1200	1200
TDP (Watt)	275	130	275	120	150	75	120	185

4.3 Ethereum Mining with NVIDIA GPUs

Graphics cards with NVIDIA chipsets are often preferred in Ethereum mining. Their lower power consumption and easy operation enable them to be preferred over AMD graphics cards. However, the more expensive the prices and the more customizable are the disadvantages. The NVIDIA graphics cards to be introduced will be GTX1060, GTX1070, and GTX1080.

Table 4.2: Factory settings of NVIDIA GPUs

	GTX 1060	GTX 1070	GTX 1080
GPU Core (MHz)	1784	1771	1822
GPU RAM (MHz)	8008	8008	10008
GPU Supply (mV)	900	1000	1000
TDP (Watt)	120	150	180

4.4 Optimization Methods

The mining performance of graphics cards can be increased by using some techniques. As the number of processes handled per second increases, it will be possible to earn more of the electric energy used by the card as crypto money. For this reason, these techniques should be applied to each card and it should be revealed how much they notice by measurements. Because each card is different from the quality level of the chip, it is possible to get better results on some cards, while it is possible to face lower performance on some cards of the same model.

4.4.1 Power Limiting

Power limitation is a very useful optimization process that can be used on both NVIDIA and AMD graphics cards. When designing graphics cards by designers, a certain amount of power consumption values are taken into account in order to avoid unstable conditions. So the power drawn by the card is actually more than necessary. This is done to prevent possible instability. If the card is to be used for game purposes, power limitations may not be required. Because it's not always possible to play games all day long. But when it comes to crypto-money mining, there is a constant effort. In this case, every watt to be drawn will be a parameter that can affect the profit-loss balance for the miner. Power limitation can be done with the MSI Afterburner program, which supports almost any card. In this study, the screenshot of the program used in version 4.6 is given in Figure 4.2.

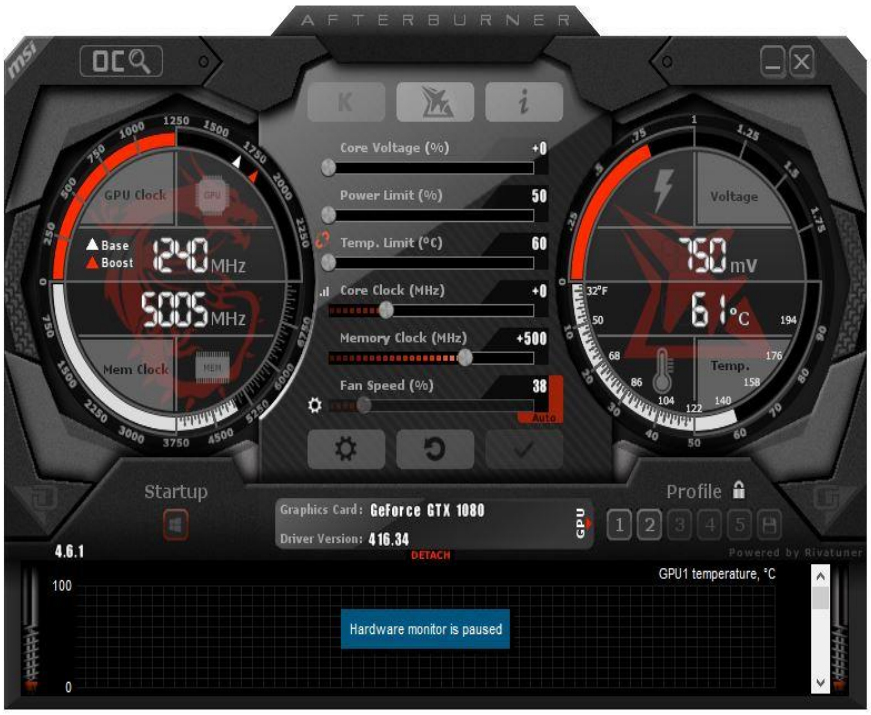


Figure 4.2: MSI Afterburner program interface

Using this parameter, the power rating should be reduced gradually and the proper operation of the cards should be observed for approximately 10 minutes. Then there will be less chance of a problem. All cards have a power limitation. This is roughly 35% fixed on NVIDIA cards and around 20% on AMD cards. As the voltage reduction process on AMD cards will also be applied, the power limitation process has not been extended much. In order for the card to run continuously without any instability, it is necessary to combine these techniques with long experiments and to obtain the best performance.

4.4.2 VRAM Timing Modification

In this study, graphics cards with GDDR5 model RAM are used. The GDDR5 model RAMs have various timing values and are separate for each card. Figure 4.3 shows the RAM delay and timing parameters of the AMD graphics cards. RAM timing values cannot be modified due to their lock on NVIDIA graphics cards. It is possible to easily optimize these timing and delay values with the 1.7.2 version of Polaris BIOS Editor. First, the BIOS information of the graphics card is saved as a new file to the desktop with the GPU-Z program. Figure 4.3 shows the GPU-Z program interface.

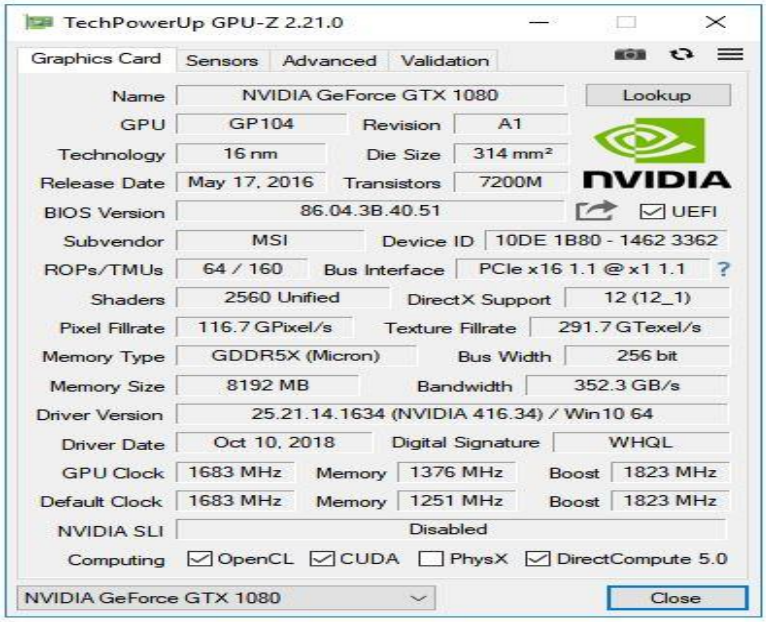


Figure 4.3: GPU-Z GPU info tool

This new file is then opened with the Polaris BIOS Editor program and processed by pressing the One-Click Timing Patch button on the bottom right. Figure 4.4 shows the Polaris BIOS Editor program interface.

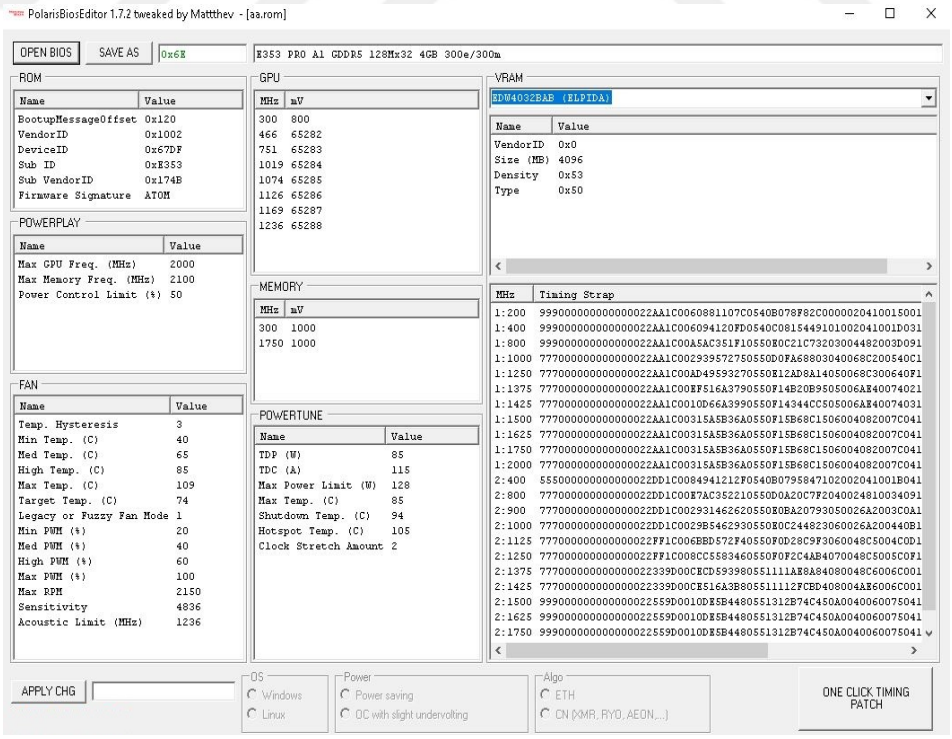


Figure 4.4: Polaris BIOS editor for AMD graphics cards

The BIOS file that is modified by the program that offers separate optimization for each card is saved and the program called AMD Windows BIOS Flashing tool is again programmed into the graphics card. Figure 4.5 shows the AMD Windows BIOS Flashing program interface.

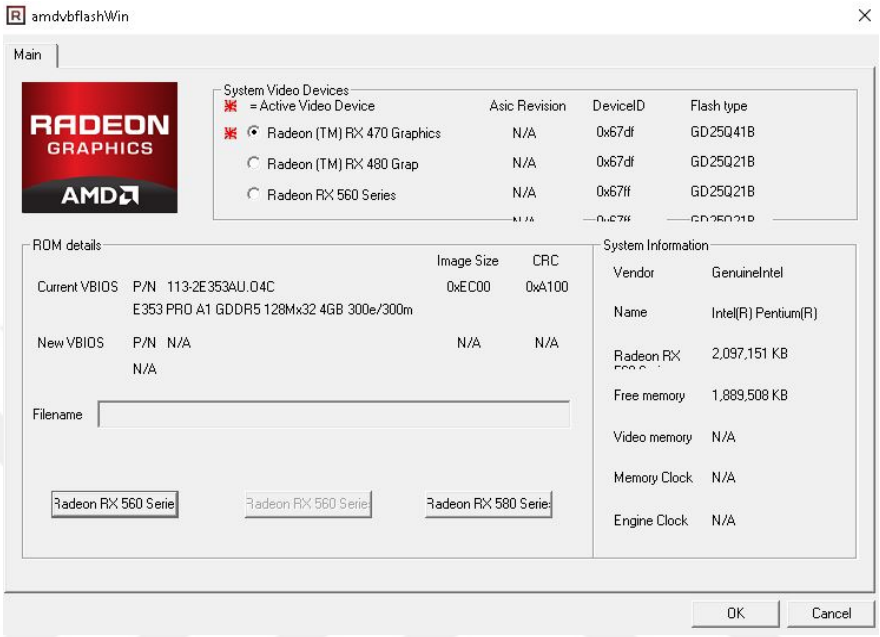


Figure 4.5: Windows BIOS flashing tool for AMD graphics cards

This optimization does not damage the card and does not spoil the warranty.

4.4.3 Undervolting and Core Underclocking

Decreasing the supply voltages of the processor and RAM on AMD graphics cards in a way that doesn't cause any instability, saves considerable power. The CPU and RAM supply voltage, which is generally determined as 850 mV, does not cause any instability and saves around 10 percent power. This can be done with a program called OverDrivenTool. The clock frequency of the processor with the program shown in Figure 4.6 can also be reduced. The 1050 MHz processor speed affects up to 10 percent power savings, minimizing mining performance. NVIDIA graphics cards cannot be interrupted because the supply voltages and processor clock frequencies are locked.

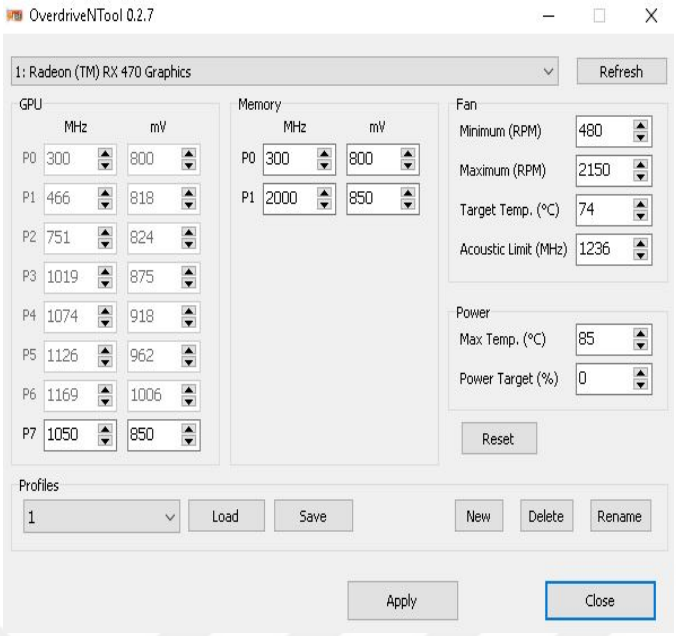


Figure 4.6: OverDrivenTool for AMD graphics card voltage modifications

4.4.4 VRAM Overclocking

Increasing the working frequency of RAM provides significant performance improvement especially in Ethereum mining. Overclocking can be performed at speeds varying on each graphics card, and this speed increase is usually between 200 and 600 MHz. This process can be done easily with the MSI Afterburner program. Step-by-step in 50MHz steps it is appropriate to increase the speed and observe the operation and performance of the card. Default frequency and voltage values are shown in Table 4.1 and Table 4.2. After optimization processing, the increases are given in Table 5.1. These increases do not increase the power consumption but increase the average speed by 5 percent.

4.5 Application of Optimizations for RX580 and GTX1080 Graphics Cards

The optimization techniques described in the previous section will be explained in this part. The RX580 4 GB and GTX1080 8 GB graphics cards are selected to show clearly the application of the optimization process.

4.5.1 Optimizations Application for AMD RX 580 4GB Graphics Card

The optimization process of the RX580 4GB graphics card which was produced by Sapphire using AMD chipset will be explained clearly in this part. Firstly; mining speed, power consumption, and mining profit will be obtained of the RX580 4GB graphics card by using several hardware and software tools before the optimization applications given in the 4th chapter of this thesis are applied. Claymore 14.7 program was used for Ethereum mining and when the program was run, the card mined Ethereum at a speed of approximately 24 Mh/s as shown in Figure 4.7.

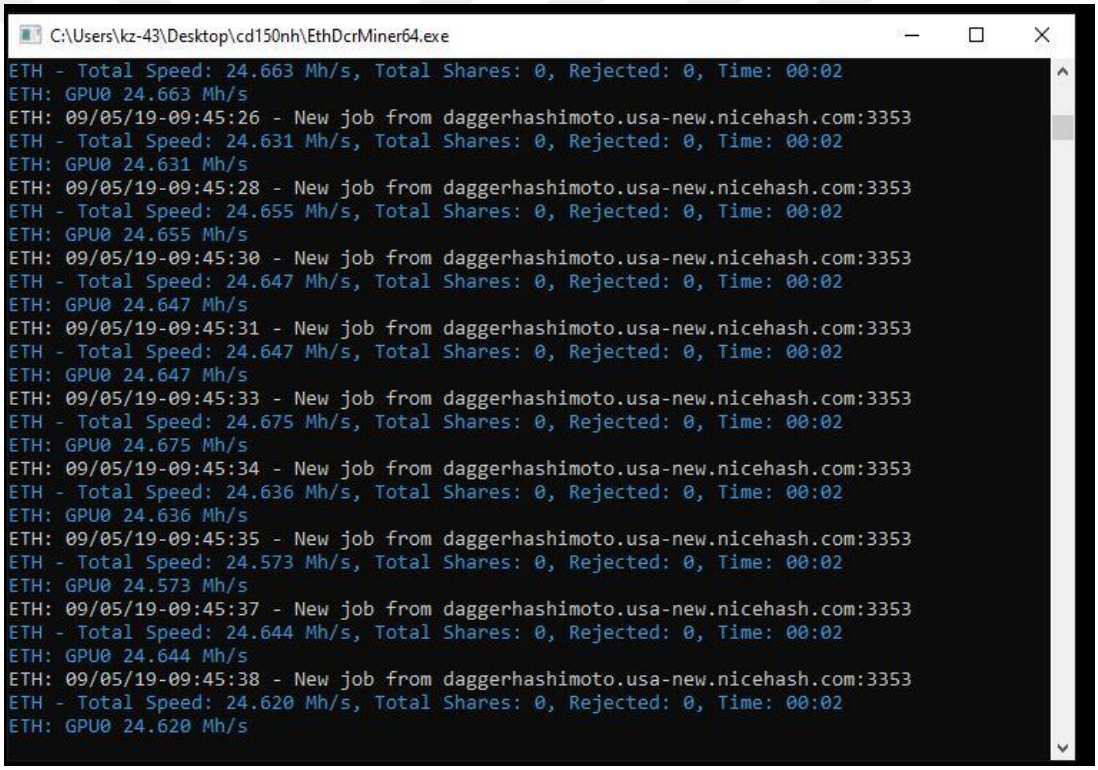


Figure 4.7: Hash rate of RX580 4GB graphics card without optimizations

After the hash rate is inspected from the console of the program, the mining profit can be calculated. Hash rate value of the card that is 24 Mh/s is entered to https://www.whattomine.com address where the profits from the mining process can be calculated easily. The power section of the calculation tool of the web site is filled with 185 Watt that is the consumed power of the non-optimized card. The current 1 kWh price of the electrical energy is 0.618 Turkish Lira is added to the cost section by

converting it to USD. At the time of writing this thesis, 1 USD corresponds to 5.7 Turkish Liras. In this case, 1kWh energy price is calculated as 0.108 USD. In the fees section of the tool, it is filled with 2 percent which is the commission of the mining program and the pool where the mining process is performed. Finally, the calculation is completed by pressing the calculate key on the right side of the web site. Monthly earnings are seen as 9.57 USD. However, since the electricity cost is calculated as 14.39 USD if the card is used in the mining process without optimizations, it causes a loss of 4.82 USD per month. The image of the site where the calculations for RX580 4GB are made was given in Figure 4.8.

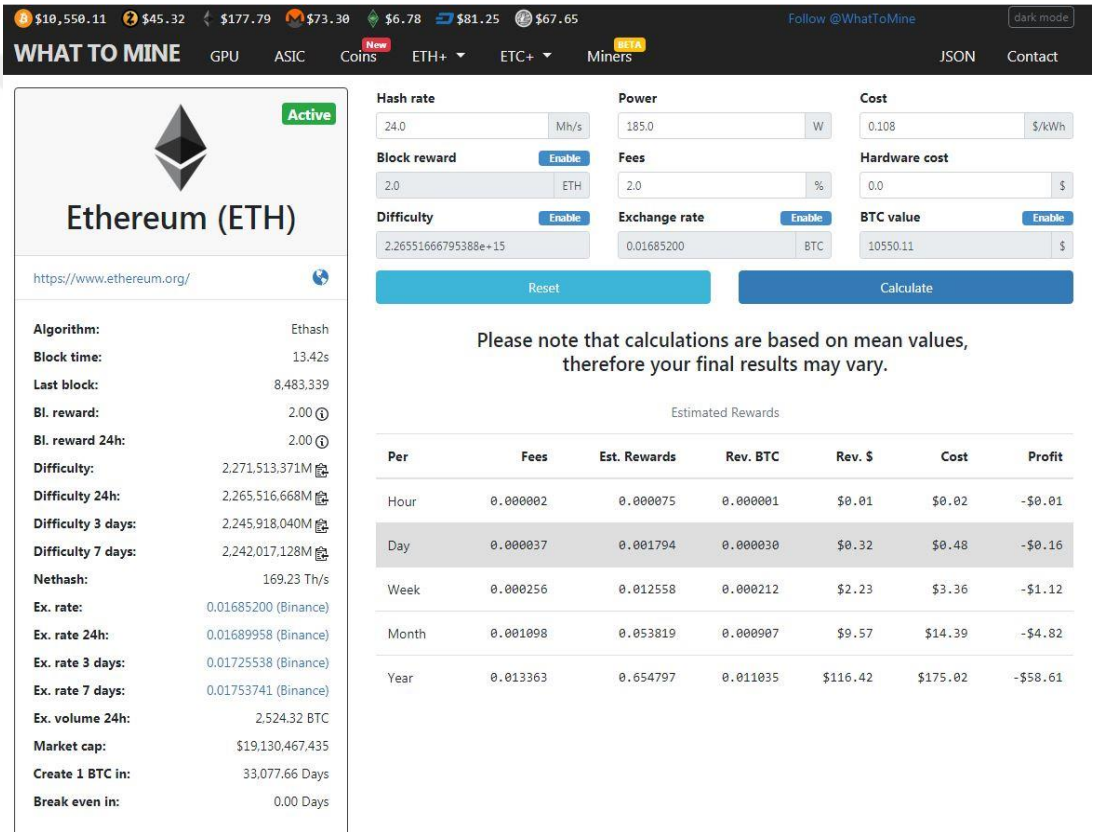


Figure 4.8: Profit calculation of RX580 graphics card without optimizations

At this stage, the optimizations described in Chapter 4 of this thesis will be applied to the RX580 4GB graphics card. These optimizations are power limiting, VRAM timing modification, undervolting and core underclocking, and VRAM overclocking.

In order to perform VRAM timing modification, first run the GPU-Z program, after that retrieve and save the BIOS ROM file as described in section 4.4.2. This file is then

processed with the help of the Polaris BIOS Editor program to obtain a ROM file with reduced RAM latencies. Lastly, with the help of the AMD Windows BIOS Flashing Tool, a modified ROM file was injected into the card. Now the RAM delays of the graphics card are reduced as much as possible.

The Overdriventool program is then used to overclock VRAM. Ethereum is memory intensive algorithm and memory speed is very important to solve equations fast and correct. On the graphical user interface of the program, values from P0 to P6 in the GPU header was deactivated. In P7, 1050 MHz and 850 mV were written. This reduces the GPU core speed to 1050 MHz. In addition, the supply voltage of the GPU core was reduced to 850 mV. Then, at the memory header of the program, the P1 line was filled with 2000 MHz and 850 mV. The VRAM speed was increased to 2000 MHz and the VRAM supply voltage was reduced to 850 mV. Reducing the supply voltages is allowing the card to consume less electrical energy. In this way, a total of 3 optimization applications were made. After these applications, the Claymore 14.7 program was run again. As shown in Figure 4.9, it was observed that the mining speed increased to approximately 29 Mh/s and the power meter showed 130 Watts.

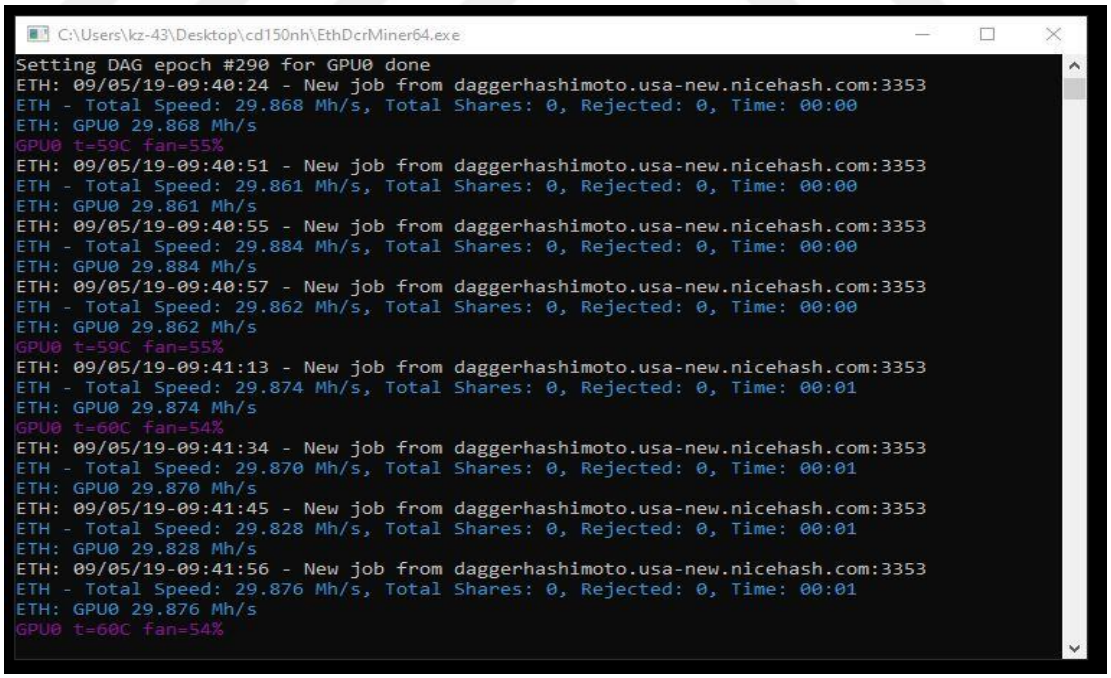


Figure 4.9: Hash rate of RX580 graphics card with optimizations

After the optimizations were made, the revenue was recalculated with 29 Mh/s mining speed and 130 Watt power consumption. As shown in Figure 4.10, gross revenue increased to 11.56 USD per month. The cost of electricity decreased to 10.11 USD per month. The monthly profit is 1.45 USD. In conclusion, these show that optimizations are proposed in this thesis are useful to get profit from RX580 4GB Graphics Card by mining Ethereum.

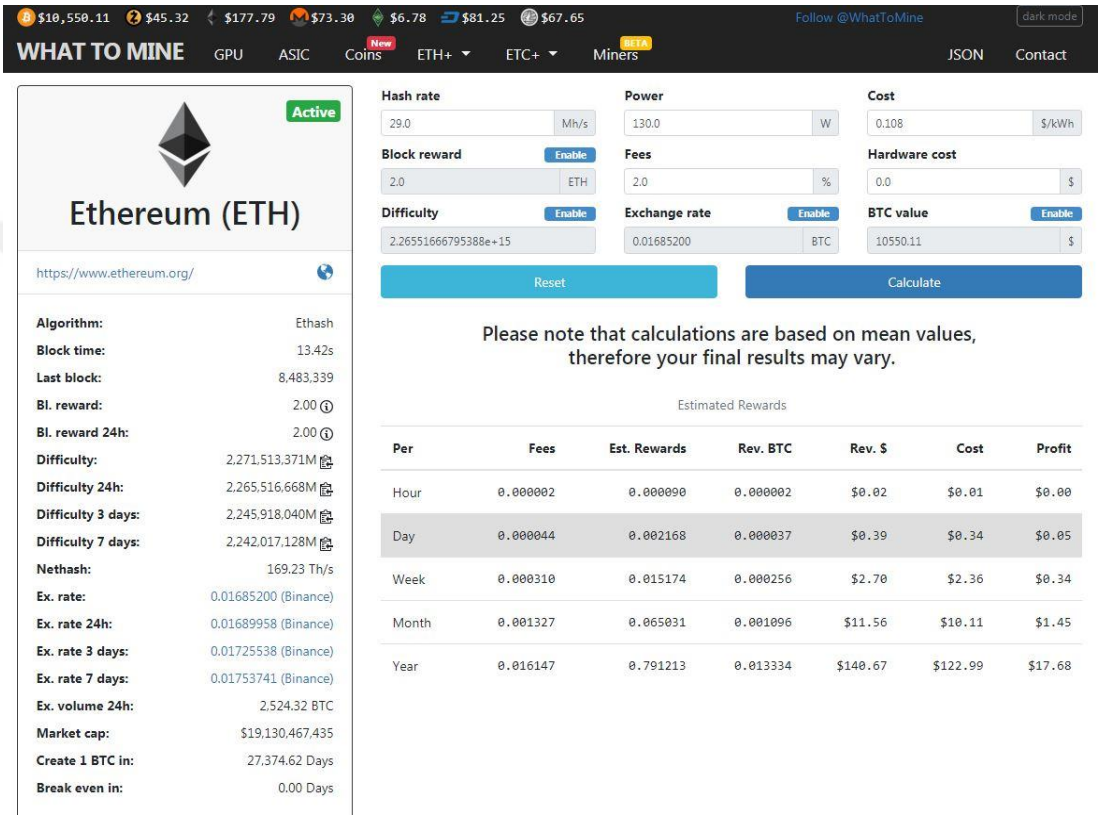


Figure 4.10: Profit calculation of RX580 graphics card with optimizations

4.5.2 Optimizations Application for NVIDIA GTX 1080 8GB Graphics Card

In this part, it will be explained clearly how to optimize the GTX1080 8GB graphics card produced by MSI using the NVIDIA chipset. Firstly; mining speed, power consumption, and mining profit will be obtained of the GTX1080 8GB graphics card before the optimization applications given in this thesis are applied. Claymore 14.7 program was used for mining and when the program was run the card mined Ethereum at a speed of approximately 28 Mh/s as shown in Figure 4.11. Secondly, the profit

calculation has to be made by using the website mentioned above. Hash rate value 28 Mh/s was entered to https://www.whattomine.com where the earnings from the mining operation can be easily calculated. 200 Watt is entered into the power section, which is the power consumption of the non-optimized card. The current electricity kWh price is 0.108 USD. In fees, a 2 percent value, which is the commission of the mining program and the pool where the mining process is performed, was entered. Finally, it was pressed the Calculate key.

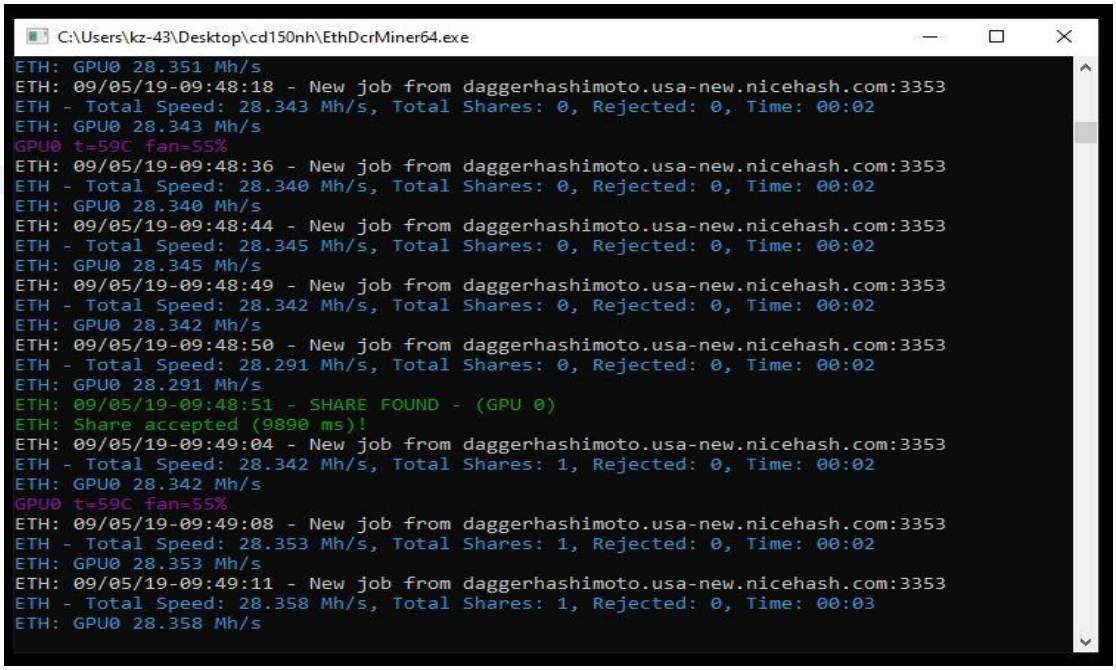


Figure 4.11: Hash rate of GTX1080 graphics card without optimizations

According to the calculation tool, monthly revenue is 11.16 USD. However, since the cost of electricity is calculated as 15.55 USD if the card is used in the mining process as it is, it causes a loss of 4.39 USD per month. The image of the site where the calculations are made is given in Figure 4.12.

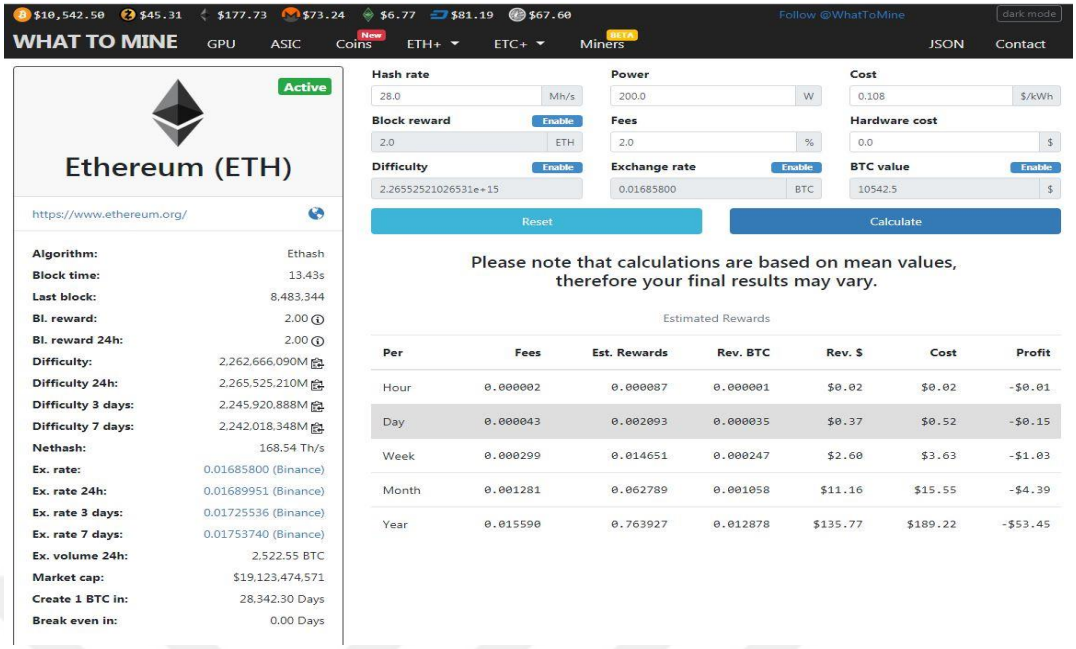


Figure 4.12: Profit calculation of GTX1080 graphics card without optimizations

At this stage, the optimizations described in Chapter 4 of this thesis will be applied to the GTX1080 8GB graphics card. These are power limiting and VRAM overclocking. VRAM timing modification cannot be applied on cards using the NVIDIA chipset. Instead, power limiting is performed by using the MSI Afterburner program. Using MSI Afterburner 4.6.1, the power limit is reduced by up to 65 percent. This will allow the card to reduce the supply voltage in itself. Then MSI Afterburner 4.6.1 is used to overclock VRAM. RAM speed is increased up to 10600MHz by adding an extra 300 MHz. This value is the highest determined stable value. After these improvements, the Claymore 14.7 program is run again and as shown in Figure 4.13, the mining speed has increased to approximately 34 Mh/s and the power meter readings have decreased to 110 Watts.

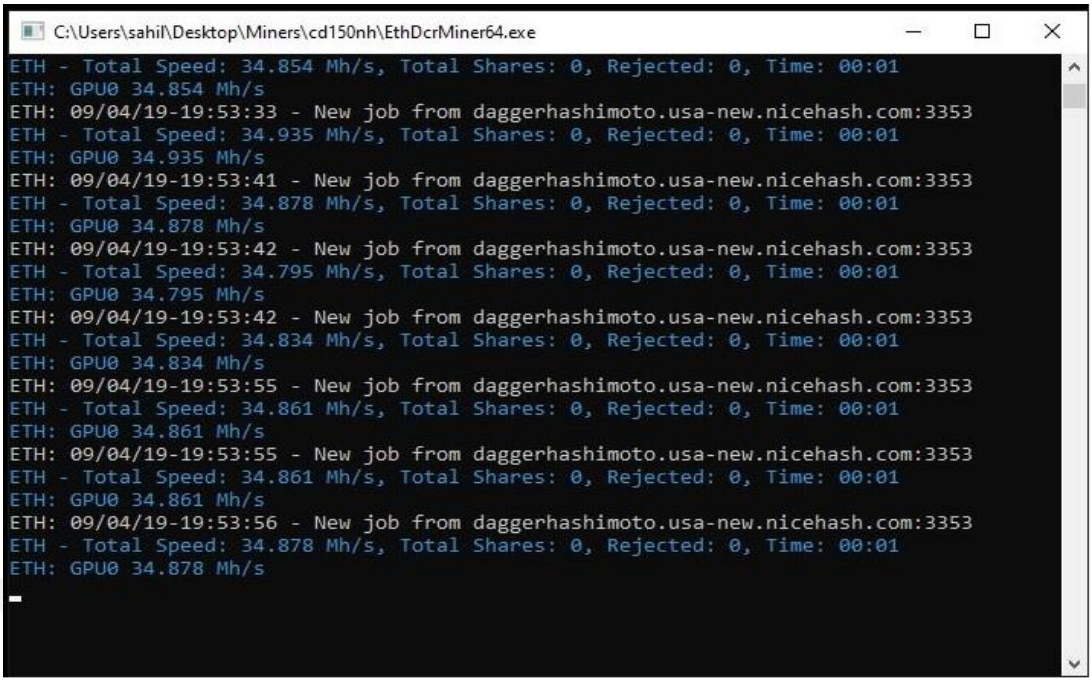


Figure 4.13: Hash rate of GTX1080 graphics card with optimizations

After both optimizations were made, the profit was calculated again with a 34 Mh/s mining speed and 110 Watt power consumption. As shown in Figure 4.14, gross earnings rose to 13.55 USD per month. Electricity costs have dropped to 8.55 USD per month and the profit is 5.00 USD.

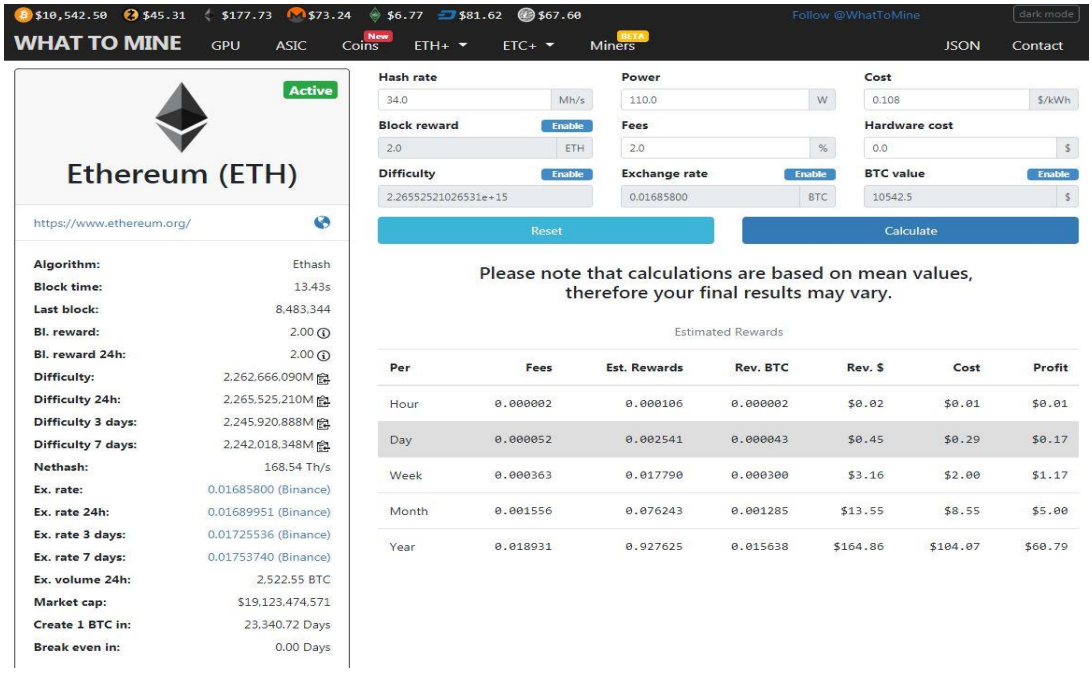


Figure 4.14: Profit calculation of GTX1080 graphics card without optimizations

CHAPTER 5

CONCLUSION

In this study, the core supply voltages of the graphics cards have been reduced in different amounts for each card and the appropriate values have been determined by taking into consideration the power consumption and the algorithm speed. These values are shown in Table 5.1. The techniques of changing the memory timings, increasing the graphics card GPU and RAM speeds, reducing the power limit and reducing the processor supply voltage were applied to each card, and the excavation speed and power consumption measurements were made. The measurement device is used in Table 4.1 and Table 4.2. In order to make a comparison, the measurements of the graphics cards in the factory settings are also made. For example; The stock rate of the AMD RX 570 graphics card was measured at 23 MH/s. In this case, the power consumption was measured at 120 Watts and the card was able to mine 0.002326 Ethereum per day. The daily income was 0.23 USD and the energy cost was 0.28 USD. In the case of ex-factory, the mining loss of the card 0.05 USD per day. When the same card was improved with the techniques proposed in this study, the mining speed was measured as 29 MH/s and the power consumption was 90 Watt. In the improved state, the AMD RX 570 can mine 0.003011 ETH per day. The daily income was 0.29 USD by using the BTC value as 100000 USD and the energy cost was 0.21 USD. In this case, the mining profit was calculated as 0.08 USD per day. The most important aim of this study is to apply optimization methods in the Ethash summary algorithm which is specific for Ethereum mining. For this purpose, improvements have been made to enable AMD and NVIDIA chipset graphics cards to solve faster algorithms with lower power consumption. In the study, Ethereum, which has an instant price of 260 USD and kWh unit price of electricity is 0.1 USD. When the graphics cards were operated with the factory default settings, none of them could profit from the current exchange rates. RX 470, RX 570, GTX 1060, GTX 1070 and GTX1080 cards were found to be in the snow zone when improved with the techniques proposed in this study. Table 5.1

shows the measurement results of the stock and modulated cards of all the graphics cards and the daily amounts of profit obtained.

Table 5.1: Results of measurement

		Bios Mod.	Hash Rate (MH/s)	GPU Over Clock (MHz)	RAM Over Clock (MHz)	GPU Under Volt (mV)	Power Limit	Diss. Power. (Watt)	Revenue (USD/Day)	Electricity Cost (USD/Day)	Profit (USD/Day)
AMD	Stock	X	22.4	0	0	0	%100	275	0.23	0.64	-0.41
R9 290	Mod.	X	27	+100	+200	-70	%80	180	0.27	0.42	-0.14
AMD	Stock	X	19.5	0	0	0	%100	150	0.20	0.35	-0.15
R9 380	Mod.	X	21	+100	+150	-80	%80	130	0.21	0.30	-0.09
AMD	Stock	X	24	0	0	0	%100	275	0.24	0.64	-0.40
R9 390	Mod.	✓	28	+100	+150	-50	%80	170	0.28	0.40	-0.12
AMD	Stock	X	10	0	0	0	%100	75	0.10	0.17	-0.07
RX 560	Mod.	✓	14	+100	+350	-90	%80	60	0.14	0.14	0
AMD	Stock	X	23	0	0	0	%100	120	0.23	0.28	-0.05
RX 470	Mod.	✓	29	+100	+350	-150	%80	100	0.29	0.23	0.06
AMD	Stock	X	24	0	0	0	%100	150	0.24	0.35	-0.11
RX 480	Mod.	✓	30	+100	+300	-150	%80	110	0.31	0.26	0.05
AMD	Stock	X	23	0	0	0	%100	120	0.23	0.28	-0.05
RX 570	Mod.	✓	29	+100	+300	-150	%80	90	0.29	0.21	0.08
AMD	Stock	X	24	0	0	0	%100	185	0.24	0.43	-0.19
RX 580	Mod.	✓	29	+100	+300	-150	%70	130	0.29	0.30	-0.01
NVIDIA	Stock	X	20	0	0	0	%100	120	0.20	0.28	-0.08
GTX1060	Mod.	X	22	+100	+600	0	%65	70	0.22	0.16	0.06
NVIDIA	Stock	X	24	0	0	0	%100	160	0.24	0.37	-0.13
GTX1070	Mod.	X	30	+100	+600	0	%65	90	0.30	0.21	0.09
NVIDIA	Stock	X	28	0	0	0	%100	200	0.28	0.47	-0.18
GTX1080	Mod.	X	34	+100	+300	0	%65	110	0.35	0.26	0.09

Reducing the power consumption along with increasing the speed of the algorithm has been an important factor in the transition to the snow zone. When compared to AMD graphics cards, NVIDIA graphics cards are currently in the process of producing more solutions in Ethereum mining for less power. In the future study, it is thought to add crypto coins such as Ravencoin, Bitcoin Gold and Monero with different algorithms from Ethereum. In addition, it is planned to continue with the efforts to increase profit in the field of algorithms from Ethereum. In addition, it is planned to continue with the efforts to increase profit in the field of cryptocurrency, by writing software that allows the instantaneous exchange of crypto money.

REFERENCES

[1] Antonopoulos, A.M., Mastering Bitcoin, USA: O'Reilly Media. 2014

[2] http://www.economist.com/news/finance-and-economics/mining-digital. Retrieved September, 03, 2019.

[3] Antonopoulos, A.M., G. W., Mastering Ethereum, USA: O'Reilly Media. 2018.

[4] Casino, F. Dasaklis, T. K. and Patsakis, C. A systematic literature review of blockchain-based applications: Current status, classification and open issues. Telematics and Informatics, 36, 55-81. 2018.

[5] Rosic A. *What is Ethereum?* Retrieved September, 04, 2019 from https://blockgeeks.com/guides/ethereum

[6] Oberhaus D. *What is an ASIC Miner and is it the future of crypto currency?* Retrieved September, 04, 2019 from https://www.vice.com/en_us/article/3kj5dw/what-is-an-asic-miner-bitmain-monero-ethereum, 2018.

[7] Nakamoto, S., Bitcoin - *A Peer - to - Peer Electronic Cash System*, Retrieved September, 04, 2019 from https://bitcoin.org/bitcoin.pdf. 2016.

[8] https://coinmarketcap.com/currencies/bitcoin/#charts, Retrieved September, 12, 2019.

[9] https://medium.com/ignation/pulling-the-blockchain-apart-the-transaction-life-cycle-7a1465d75fa3 Retrieved September, 04, 2019.

[10] https://blockchain.coinmarketcap.com/chain/bitcoin, Retrieved September, 12, 2019.

[11] ANSI, X9.62: 2005: The Elliptic Curve Digital Signature Algorithm (ECDSA), Public Key Cryptography for the Financial Services Industry, 2005.

[12] Johnson, D., Menezes, A. and Vanstone, S. The Elliptic Curve Digital Signature Algorithm (ECDSA), International Journal of Information Security, 1, 36-63. 2001.

[13] https://coinmarketcap.com/currencies/ethereum/#charts, Retrieved September 04, 2019.

[14] https://80000hours.org/podcast/episodes/vitalik-buterin-new-ways-to-fund-public-goods/. Retrieved September, 04, 2019.

[15] https://blockchain.coinmarketcap.com/chain/ethereum, Retrieved September, 04, 2019

[16] Justin Fisher, Maxwell Henry Sanchez, Authentication and verification of digital data utilizing blockchain technology, United States, 2016.

[17] https://allprivatekeys.com/, Retrieved September, 04, 2019.

[18] https://medium.com/pillarproject/the-pillar-wallet-current-state-and-the-vision-for-2019-69f85d866cb0. Retrieved September, 04, 2019.

[19] https://amturing.acm.org/award_winners/diffie_8371646.cfm, Retrieved September, 04, 2019

[20] Ready, Y. *Signing and Verifying Ethereum Signatures*. Retrieved September, 12, 2019, from https://dzone.com/articles/signing-and-verifying-ethereum-signatures. 2018

[21] https://etd.lib.metu.edu.tr/upload/12607698/index.pdf, Retrieved September, 04, 2019.

[22] Heide, D. T. *A closer look at Ethereum signatures*. Retrieved September, 12, 2019 from https://hackernoon.com/a-closer-look-at-ethereum-signatures-5784c14abecc. 2018

[23] *National Institute of Standards and Technology (NIST), SHA-3 Standard*, Retrieved September, 12, 2019 from https://nvlpubs.nist.gov/nistpubs/FIPS/NIST.FIPS.202.pdf. 2018.

[24] https://en.bitcoinwiki.org/wiki/SHA-3, Retrieved September, 13, 2019.

[25] Advances in Cryptology, 12th Annual International Cryptology Conference Santa Barbara, California, USA August 16–20, 1992.

[26] https://en.wikipedia.org/wiki/Proof_of_work#cite_note-DwoNao1992-1, Retrieved September, 13, 2019.

CURRICULUM VITAE

PERSONAL INFORMATION



Name Surname : Gizem KIZILBEY

Date of Birth : 25.10.1992

Phone : 0262 675 25 54

E-mail : gizem.kalkanci@tubitak.gov.tr

EDUCATION

High School : Adıyaman Fatih Anatolia High School

Bachelor : Ankara Yıldırım Beyazıt University

Master Degree : Ankara Yıldırım Beyazıt University

WORK EXPERIENCE

Engineering : TUBITAK – BILGEM / BTE (2017-)

Intern Engineering : TUBITAK – UZAY (June – July 2015)

Intern Engineering : TUBITAK – UZAY (July – August 2014)

Intern Engineering : TEIAS – Akköprü (June – July 2014)

TOPICS OF INTEREST

- PCI, Cryptography
- Crypto money mining

September 2019

ANKARA

Department of Electrical and Electronics Engineering

Gizem KIZILBEY