ADVANCED CRYPTO MINING STRATEGIES
HOW TO MINE CRYPTO AND A GUIDE FOR CRYPTOCURRENCY BEGINNERS

Table of Contents
Chapter 1: Introduction........................................................................................................................................8
  What is cryptocurrency? ....................................................................................................................................9
  Beginners Understanding on cryptocurrency .................................................................................................9
  History of Bitcoins and other coins. ...............................................................................................................10
  Who is Satoshi Nakamoto? ...........................................................................................................................11
  What is Bitcoin? ............................................................................................................................................11
  Brand New Bitcoin Reward ...........................................................................................................................12
  Understanding how to trade with Bitcoins .....................................................................................................12
    Understanding Steady Change of Bitcoin Price ............................................................................................13
  Breaking Complexity in Crypto Mining .......................................................................................................13
Chapter 2: How Bitcoins Works ......................................................................................................................15
  Owning a Bitcoin..........................................................................................................................................16
  Origin of Bitcoin Addresses ..........................................................................................................................16
  Bitcoin Transactions....................................................................................................................................16
  Working of Blockchains................................................................................................................................17
  Can Bitcoin be Created out of Thin Air? ........................................................................................................17
Chapter 3: Bitcoin Mining and Consensus ........................................................................................................18
  Securing and synchronizing blockchain by mining.........................................................................................18
  Abuse of Bitcoin............................................................................................................................................19
  Why has Bitcoin become very controversial over the years? .......................................................................19
  Bitcoins Economics and Currency Creation..................................................................................................20
  A De-Centralized Consensus..........................................................................................................................21
  Independent Confirmation (Verification) Of Transaction ...............................................................................22
  Aggregation of Transactions into Blocks........................................................................................................23
    Transaction Fees, Age, and Priority ...............................................................................................................24
    Generation Transaction ................................................................................................................................26
Quantitative analysis.................................................................................................................. 118
Investment strategy .................................................................................................................. 118
In a nutshell .............................................................................................................................. 119
Trading With Monero ............................................................................................................. 119
Chapter 10: Tips For Mining Crypto Currency ..................................................................... 120
Tips .......................................................................................................................................... 120
A mining Rig will be the first order of the business ............................................................... 120
Get a Coin wallet .................................................................................................................... 121
Get a good mining pool .......................................................................................................... 121
Have a computer-mining program ......................................................................................... 122
Organize a VPS ....................................................................................................................... 122
Tricks ........................................................................................................................................ 122
Choose right GPU .................................................................................................................. 122
Drivers ..................................................................................................................................... 122
System ..................................................................................................................................... 123
Make rig at least 5 GPUs ....................................................................................................... 123
Use USB risers ....................................................................................................................... 123
Cool down old GPUs ............................................................................................................ 123
Edit virtual memory ............................................................................................................. 123
Chapter 11: Strategic Plan in Mining ....................................................................................... 124
Hardware Requirement .......................................................................................................... 124
The software requirements .................................................................................................... 125
Operating system updates ..................................................................................................... 125
Graphics cards software and drivers .................................................................................... 126
Mining software ..................................................................................................................... 126
Coin wallet ............................................................................................................................. 126
Configuring your miner ......................................................................................................... 126
Optimization ........................................................................................................................... 127
Video card optimization ........................................................................................................ 127
CGMiner optimization ........................................................................................................... 127
Chapter 1: Introduction

What is cryptocurrency?
Cryptocurrency is a form of digital currency created using cryptography. Therefore ‘cryptocurrency’ is a name derived from the word cryptography which means being encrypted. In simple, this can be translated directly to mean, a currency that has been verified and encrypted using a digital system. Cryptography technology boomed back in the 1980s when many digital currencies were discovered and availed broadly for use. Investing in this market was such a great risk as most people associated it with robbery, violence and drug addiction, while others thought that it was a pyramid scheme something that exists even today.

Currently, Crypto mining has become a central activity for all. It is very important to understand that cryptocurrency is deeply rooted in the high digital notch. As a result, to access this currency one should be involved in transactions that are carried using digital platforms that use the encrypted software. What the system does is that it controls currency transfer and peer-to-peer transactions without involving any central role players such as the government or the banks. The most interesting thing about the use of cryptocurrency is that it is never affected by inflation or deflation which highly stagnate the extended market using money currency. As a result, most investors opt to invest in crypto coins. An annual record of over 0.5 % increase of new crypto users is a proportional evident to the rampant increase in the mining of the cryptocurrency.

Beginners Understanding on cryptocurrency
Cryptocurrency is an ambiguous word for newbies. Much concern on writing this book is to deliver the right resources for excellent understanding on how to Crypto mine and releasing an elaborate guide to lead beginners in getting started with minimal struggle. It is important to note that Cryptocurrency is an anonymous word in the digital market that is trending at an alarming rate. The fact is that trying to understand the whole process is worth everything, bearing in mind that today; those with knowledge of digital currency are reaping abnormal profits that nobody can make in the normal money currency market.

From records of cryptocurrency statistics, a lot of improvement is taking place with so many beginners flowing in every day. Well, the future of cryptocurrency is unpredictable with most of its application seeming to be more of a fad. Not until 2017, that cryptocurrency has taken charge of the market with so many members despite the cons and the pros that might affect its future performance. To get an absolute understanding of the digital money, you are required to master the basics of cryptocurrency, majoring on its origin, who founded it, where and when among other facts concerning its history.
History of Bitcoins and other coins

Nakamoto Satoshi discovered Bitcoin mining in the year 2008. This was followed by the publication of white paper writing entitled “A Peer-to-Peer Electronic Cash System.” To create a fully decentralized and an independent electronic cash system, Satoshi relied on two major inventions that he had invented prior to the latter. That is the technology on hash cash and the B-money. Therefore, electronic cash system is a combination of the hash cash and the B-money technology. To understand the system; one should first consider establishing a foundation of knowledge about the two types of technologies. Bitcoin mining system is a digital distributed computing technology that is designed to carry out algorithm math after every 10 minutes on a global level. All that matters is that the system network is decentralized to ensure that there is a balanced consensus for the entire transaction and that double spending is avoided ensuring that there is no use of single unit twice.

After the invention of Bitcoin in 2008, the network took a whole year of testing, investigating and verifying. After that, it started operating in 2009. At this time, the entire network soley depended on Sakoshi publications and guidelines after which various people started inventing other programs and revising Sakoshi work. Today, there is a record of rampant increase in Bitcoin resilience and security due to great improvement in the technological advancement of the distributed digital computation system.

According to digital currency and financial statistics, the Bitcoins electronic system processing capacity is above any top rated supercomputer in the world today. Currently, the value of Bitcoin in the market is estimated to be $150 billion which varies depending on the rate at which the dollar and Bitcoin are being exchanged. Bitcoin mining is a decentralized system; fully dependent on its computation. This means that it does not involve any central agency or authority to help in making transactions valid, settling payments or issuing of currency among the transacting individuals. The system relies on a proof of work as an indicator that certain transaction took place and that a certain individual upon success earned some brand new Bitcoins. Today, the bitcoin electronic system can instantly process over $150 and release them freely for the peer-peer transaction at a zero cost. No charges are made in such transactions since no middle-man is involved. Additionally, no taxation occurs on this system of transaction.
Who is Satoshi Nakamoto?
The person who invented the Bitcoin decentralized electronic system is not known by anyone even though most people refer him as Satoshi Nakamoto. In fact, the name Satoshi Nakamoto represents an alias that discovered Bitcoin currency; published white paper writing entitled “A Peer-to-Peer Electronic Cash System” for decentralized transactions. They provided an encrypted Bitcoin mining software for mining devices as well as an inbuilt mining procedure that is transparent among those doing the transactions. They laid a great foundation about Bitcoins, developed it and made it usable to people with the aim of having a decentralized currency. This was majored in boosting the economy through eliminating the central banks. Unfortunately, since April 2011, Satoshi Nakamoto disappeared and was no longer heard in this industry. Amazingly, a group of people interested in peer-peer transactions joined hands and developed a cryptocurrency networks of Bitcoins and codes for the system. So far, it is clear that not even the developers can control the system since it is fully designed to operate under mathematical computation principles, which have been made open and transparent to everyone. This provides a guaranteed assurance that nobody can earn at the expense of another person.

Therefore, the invention is basically designed to greatly benefit those that have a superb understanding of econometrics and economics as well as the ability to work out distributed computations using software installed device. A practical ability in coming up with solutions for emerging problems concerning math computation is highly demanded among the transacting peers. Satoshi Nakamoto work on an attempt to provide solutions for computing problems has been of great importance to the wider decentralized networks. This knowledge has therefore helped in winning lotteries, making registration of assets, conducting fair elections as well as in enhancing digital notarization among others.

What is Bitcoin?
In an ecosystem of digital currency, a combination of technology and concepts under which transactions operate is what is referred as Bitcoin. It is a measured unit of currency that is used to transmit and store a value from one peer to another during transactions, hence forming Bitcoin networks. Internet is the major network through which the bitcoin networking takes place. There are other networking methods for the partners to keep transacting regardless of locations and
distance. The whole Bitcoin networking can be stack on software which is easily installed in the computer of Bitcoin user.

The software can as well be installed in mobile smartphones, laptops, and the desktops in order to make the market affordable and available to all. Just like the money or any other currency used worldwide, Bitcoin currency can be used by the merchants and the ordinary people as a unit of value for sales and purchases, for crediting and debiting as well as for sending to people among others. The greatest advantage of using Bitcoin currency over money currency is that, they are universal hence can never be limited by borders. Moreover, with bitcoin currency, high security is enhanced since the system is encrypted and endowed with digital features such as digital signing. Most surprisingly, the system is faster, transmitting Bitcoins than any other currency.

**Brand New Bitcoin Reward**

Bitcoin mining involves working out hard computations with the aim of finding their solutions in order to get a new Bitcoin reward. You need to note that, the miner is a device with Bitcoin software and a stack of Bitcoin mining procedure. The device can also be referred to as the participant. The ability of mining is based on the processing power of the computer or any other device being used. The encryption system is designed in such a way that a solution for a new problem is discovered in an interval of every 10 minutes, hence making the past time valid and worth an award of new Bitcoins. The algorithm mathematics are inbuilt in the device of the Bitcoin users in order to amicably control the way in which Bitcoin networking takes place. After achieving a solution, the system adjusts automatically, and the next cycle starts. Decentralizing the issuing and currency clearing makes it possible to operate the crypto market without the need to involve middle agencies such as the government or the central bank hence enhancing global competition.

Bitcoin issuing rate is fixed. For a period of 4 years, Bitcoins created are fixed and regulated to 21 million Bitcoins; without having to exceed or be less than that by the time, we get to the year 2140. This is after dividing the total number of coins created with this specific period of time into two. Besides, the number of the participants does not matter since problem-solving is on the progress. Deflation will only occur in the Bitcoin network market when the currency issuing among the participants decreases. Since the system is regulated for specific coins within a speculated period of time, inflation may not occur in this kind of market. In fact, the addition of more Bitcoins may not affect the market since the time of solving a problem is calculated and the coins to be used are fixed.

**Understanding how to trade with Bitcoins**

Using Bitcoin requires one to have all the basic information cutting across any knowledge regarding its use. Well, this is explained in this book to ensure that your Bitcoins are secure and you are at peace with your mining. Internalizing the various explained aspects of this book will give you a full explanation concerning; winning brand new Bitcoin awards, using your Bitcoins among other. All you will require considering before taking any further step is **to have a bitcoin secured wallet**. A wallet is your bank, which should be well guarded and secured, else you may
lose everything. Among the Bitcoins wallets available to choose from include; mobile Bitcoin wallet, hardware-based wallet and the web-based wallet. Mostly some will back up there secured web-based wallets to ensure that computer hackers do not get access to their savings.

**Understanding Steady Change of Bitcoin Price**

Similar to the money market, the Bitcoin pricing may inflate or deflate with time. Though mostly, the price is moving upwards, it is important to keenly note that as time it goes down. Today, a Bitcoin is over $2100 while a year back it was $150. Changes are expected any time hence readiness is very necessary. With the current trend in the Bitcoin industry, it is expected that the value of Bitcoin will maintain the upward curve for some while though it may assume a low curve anytime soon. In fact, since the industry is growing and getting new updates, there are high expectations that in the near future the Bitcoin providers will change their service provision rules. These may include; hiking the price, stoping confirmations or increasing charging fees.

Once you transact with Bitcoins, it is not possible to do a reverse, unless your transacting partner reversed it for you. Unlike the debit and the credit cards such as the PayPal and the master cards, there is no central agency to file a claim in case you lose your Bitcoins, hence when you make your payments, make sure you double check the Bitcoin key address for confirmation.

**Breaking Complexity in Crypto Mining**

The complexity of cryptocurrency is as a result of different digital currencies, which require particular and specific understanding that varies from each other. In the pursuit to familiarize and join the digital currency market, great knowledge is necessary for choosing the right tool to help in deciding on which field to start with. This includes, getting the best device with a competitive capacity processing system, installing a cryptocurrency software and finally gathering the key knowledge on how to get started. Complexity is also experienced when determining the best trading coin. As a beginner you will encounter different digital currencies, which include; Bitcoin, Litecoin and Ethereum just to mention on the most common in the market among others. It is important to note that among other coins, Bitcoin is the most preferred by many, most common and largely trading cryptocurrency in the entire world.
CHAPTER TWO
HOW BITCOIN WORKS?
Chapter 2: How Bitcoins Works

Bitcoins have become controversial over the years as many reasons have come out to make Bitcoins a real media sensation. Between the year 2011 and 2013, many criminal organizations made Bitcoin popular by buying them in millions of dollars. They did this to keep the law enforcers out of their track.

Subsequently, demand for Bitcoins skyrocketed. Bitcoins have removed the mandate of making money from the central federal banks and placed it on the general public. Bitcoins accounts cannot be examined or frozen; by the federal government. No banks are necessary for Bitcoins to move on. Financial institutions or law enforcers cannot control Bitcoins. Bitcoins are forgery-resistant due to their intensive computation. This makes it financially unworthy to counterfeit and manipulates the system.

Bitcoin works in a way that differentiates it from other payment systems. Getting started with Bitcoin does not require a technical know-how. By just installing a Bitcoin wallet (software) on your device, a first Bitcoin address is generated and you can always create more whenever the need arises. You can share this address with friends and partners, which will enable them to transact with you. Bitcoin address is used only once.

Bitcoin software verifies and tracks transactions on a blockchain, which is a shared public ledger over a peer-to-peer network. Data and operations linked with Bitcoin are not stored in one place hence they are decentralized. Bitcoin has a network of computers all over the world that relay data to each other. Anyone can install, use and run Bitcoin software on their computer. Decentralization makes it impossible for a person or authority to control or manipulate it. No one controls Bitcoin it runs on people devices around the world.
Once you possess Bitcoins, they behave like real gold coins; have value, and they can trade like gold. You can use them to purchase goods and services online. Like money, bitcoin also can be saved somewhere in order to gain value in future. The value of a Bitcoin varies daily. This value can be checked in places like Coindesk. Currently, there are more than 2 billion worth Bitcoins that exist.

Bitcoin has no physical address, and it digitally appears as entries in a blockchain. The blockchain is the vital core data of Bitcoin. It is the database of every transaction made within Bitcoin. Devices installed with Bitcoin software keep records of transactions in the blockchain and broadcast them to other devices. Summation of these transactions determines the balance of Bitcoin users.

**Owing a Bitcoin**
For you to have a transaction greater than zero, you must be a receiver of at least one transaction stored in the public ledger. Each receiver of a transaction is identified by a special Bitcoin address. These addresses are made of numbers and letters between 27 to 34 characters. For you to own a bitcoin, you must have at least one bitcoin address. Bitcoin is obtained and sent to addresses in a manner similar to sending emails. However, bitcoin address is used only once.

**Origin of Bitcoin Addresses**
Bitcoin addresses are generated randomly by Bitcoin software running on a device. No other person or authority is involved in generating a new Bitcoin address, as the process is private. They are free and have no limitation to the number you may want to own. They have no connection to the owner identity, and no phone number, email address or username is required to obtain Bitcoin address. Bitcoin addresses are derived from two large numbers generated randomly. One is a private key while the other is a public key. In every Bitcoin address created, the Bitcoin software randomly generates a private key. A mathematical process then generates the public key from the private key. The two form a cryptographic key pair. The Bitcoin address is a simple representation of the public key.

Bitcoin addresses can be safely shared with others when you require them to send you bitcoin. The private key is always kept private. It is required to confirm ownership of public key through a cryptographic process known as digital signing. Any person with access to a private key can use or spend any Bitcoin associated with the public key. All private and public keys generated are stored in the special device file known as Bitcoin wallet. Prove of ownership and spending of a Bitcoin can only be done using the private key. Loss of a private key means all the Bitcoin linked to it cannot be spent. Note that a Bitcoin address (public address) is generated from a private key mathematically and it is the private key that is used to spend the Bitcoin.

**Bitcoin Transactions**
A Bitcoin transaction is the transfer of value between wallets of Bitcoin in a shared public ledger (blockchain). The entire Bitcoin network relies on the blockchain and everyone on the network has a copy of the blockchain. Bitcoin wallets keep seeds or private keys, which are a secret piece of
data. These private keys are used to sign transaction where they provide mathematical evidence that they originate from the owners wallet.

These signatures provide security by preventing the transactions alterations by anyone once they are issued. Each transaction is broadcasted between users through a process known as mining. For someone to receive a Bitcoin, you should provide the sender with the generated Bitcoin address. The sender sends a new transaction with their named address as the sender and receiver address as the recipient.

**Working of Blockchains**

A Bitcoin fundamentally is a very simple data ledger file known as blockchain. This is comparatively small, just like a long text message on a smartphone. A Bitcoin blockchain is made up of three parts: identifying address, history and the private key header log.

The identifying address is made up of approximately 34 characters; the history part is the ledger showing who has bought and sold it. The third part is the complex part where a complicated digital signature is captured to confirm every transaction for a particular Bitcoin file.

All devices involved in Bitcoin network maintains and stores a copy of the blockchain. After the users have spent their Bitcoins, the transactions are broadcasted to the network. The new transaction is collected. Verified and saved in the blockchain. These latest updates are grouped as data chunks known as blocks. These new blocks are broadcasted to the rest of the network for updates.

All blocks in the blockchain are stored in chronological order. Only new blocks can be added to the blockchain. The already existing blocks cannot be removed or modified. This is done using cryptographic hashing. All new entry blocks must have a hash value to prove that new block exists just after the prior block. Any tamper or modification will unpredictably manipulate the referencing hash value of all the blocks that will follow. This technique maintains the chronology of the blockchain and prevents modification or tampering with existing blocks. Synchronization of transaction and barring of dishonest users is done using public key cryptography and the concept of proof-of-work.

**Can Bitcoin be Created out of Thin Air?**

Every Bitcoin exists as an entry in the blockchain ledger. These entries describe transactions from sender to recipient. All senders must first be recipients of an existing transaction. For you to be a sender, you must first be a receiver, and this is confirmed or verified using the digital signature. Note that existence and ownership of Bitcoin is only because of a transaction. However, the sole exception to the sender to recipient rule is the transaction that describes newly made Bitcoin (mining). In these transactions, there are no senders only recipients exist. Note that Bitcoins cannot be counterfeited as they can be traced up to their origin.
Chapter 3: Bitcoin Mining and Consensus

Bitcoin consensus is a distributed consensus system, which is used to confirm a waiting transaction by adding them in the blockchain. Bitcoin mining can also be defined as the process of adding transaction data record to the Bitcoin public ledger of previous transactions. It puts a chronological order to the blockchain, allows other computers to agree on the state of the system, and offers the neutrality of the networks. For a transaction to be confirmed, it should be packed in a block that fits a very strict cryptographic rule which is verified by the network.

These cryptographic rules prevent previous blocks from modifications, as this would invalidate all incoming blocks. Mining prevents individuals from adding new blocks in the blockchain. By this, no person can control what has been added to the Blockchain, redo parts of the blockchain, or get back what they have spent.

Mining is a competitive application of computational power in calculating numerical that fall within a prescribed range. Occasionally, the validated number is adjusted by the Bitcoin network to make it difficult to find its solution. The target solution is usually one solution every ten minutes. The numeric solution should be cryptographically computed and confirmed based on the latest set of transaction and the last block on the blockchain, hence creating a solution that is unpredictable and different from each competition.

Brand new bitcoins are awarded to the first miner to come up with a numeric that fits the criteria. An additional fee is deducted from transaction paid by other people sending Bitcoin in the Network. The Bitcoin software adjusts the competition such that there are only six winners per hour. This creates a limitation on the number of Bitcoins that can be created. Also, the amount of Bitcoin created in every competition, is halved; for every 210,000 competition.

Securing and synchronizing blockchain by mining

A digital signature is used to verify the amounts and senders of transactions. More so, it captures and confirms each transaction for a particular Bitcoin file. Every digital signature is unique for every individual user and their personal Bitcoin wallet. They are the security systems for the Bitcoins. Each transaction of Bitcoin blockchain is tracked and disclosed to the public. After that it is attached with a digital signature as a confirmation. The signatures are scanned for some seconds across the network to prevent duplication of the transaction and forgery of Bitcoins involved in the transaction.

However, digital signatures cannot prevent conflicts of new transactions trying to spend the same Bitcoin. Bitcoin solves the problem of double spending by a method called proof-of-work. When
a miner wins a competition, he/she publishes the result. This includes most recent validated transactions that they have collected in the network as a block for blockchains.

This block is sent in the whole network, and other users receive and verify it. The valid proof-of-work is the solution to the mining problem by a miner.

The number that solves a competition is very difficult to calculate. Nevertheless, once it has been known it becomes easy for other Bitcoin users to verify it and this is the key concept of proof-of-work. In some occasion, two miners can send a solution to a block at the same time. This causes what is known as a fork in the blockchain. Users might accept both block and their track. Sometime later a new block is solved and added to either of these blockchains. This makes it become longer than the others. Hence miners will prefer it in reference to the shorter one. The shorter blockchain will remain unconfirmed.

In such a case of multiple blockchains, users in the Bitcoin network will deem the longest blockchain as the valid one. A general agreement states that; once a chain is six blocks deep in the blockchain, its confirmation cannot be reversed.

**Abuse of Bitcoin**

Bitcoin can be abused in three major ways;

- The time delayed in confirmation; (technical weakness). On rare occasions, Bitcoin can be used twice at the confirmation interval. Due to peer-to-peer travel of Bitcoin, it can take several seconds for a confirmation to be transmitted between peer-to-peer networks of Bitcoin users. At such an instant, a fast clicking dishonest person can submit a second transaction of the same Bitcoin to another recipient. However, the Bitcoin system will eventually identify the double spender. Unfortunately, if the recipient had transferred goods before confirmation, they will lose both the goods and the payment.

- Pool organizers taking shares which are not fair; (Human, dishonesty). Since Bitcoin mining is best attained through joining thousands of miners (pooling), it is the organizers of the pools who decide on how the achieved Bitcoins will be shared. These organizers can decide to take lion shares at the expense of the others.

- Online exchanges; (human mismanagement). Online exchangers that trade Bitcoins for money may be incompetent or dishonest. In conventional banking, users are partially insured against loses, but in Bitcoin exchange, such does not exist.

**Why has Bitcoin become very controversial over the years?**

Several reasons have made Bitcoin become such a big deal. Here are some of the reasons.

- Bitcoin is neither made by any central federal bank nor are they regulated by any government.
There are no banks tracing money movement, government tax agents or law enforcers. Uncontrolled money movement is a problem to government policing and taxation. Bitcoins have become equipment for money laundering and contraband trade which has resulted in increased Bitcoin demand among the wealthy international criminals. Therefore the value of Bitcoin has increased overwhelmingly.

- Bitcoins wallets have no limitations for spending or withdrawals. They cannot be audited, frozen or seized by banks. Only the owner of the wallet has control over it.
- Bitcoin is changing how we spend and store our money. The power to handle money is mostly done by various banks and central mint. The banks print, store and transfer money at a fee. When these banks need more money, they print or add more digits in the electronic ledger. This system is easily gamed or abused by banks. Checks are simply a promise to have value; they do not have a physical backup like gold.

Bitcoins allow the owners to have control of their money. They are not virtual bank balances which promise value. Instead, they are complex data packages that have value within themselves.
- Bitcoins transactions are actually irreversible. Most conventional payments are insured and reversed by the involved banks. However, as for the Bitcoins, any transaction is final. It has no insurance protection hence when the wallet hard drive is lost or the wallet password, whatever was in the wallet will never be recovered.

**Bitcoins Economics and Currency Creation**

As discussed previously, Bitcoins are created at a fixed and diminishing rate. Bitcoin creation process is called mining. This is because it’s rewarding is made in such a way that it stimulates a diminishing return, similar to mining of precious metals. The amount of new Bitcoins a miner can supply to a block declines approximately every four years. It started in January 2009 at 50 Bitcoins per block. In November 2012 it had halved to 25 Bitcoins per blocks and 12.5 Bitcoins per block in 2016. The Bitcoin production will declines exponentially until approximately 2140 when all the possible 21,000,000 Bitcoins will be generated. At this point, no blocks will have new Bitcoin. Miners will get their rewards only through transaction fee.
Let us look at an example below and to calculate the total number of Bitcoins that will be generated.

```python
# Original block reward for miners was 50 BTC
start_block_reward = 50
# 210000 is around every 4 years with a 10 minute block interval
reward_interval = 210000

def max_money():
    # 50 BTC = 50 0000 0000 Satoshis
    current_reward = 50 * 10**8
    total = 0
    while current_reward > 0:
        total += reward_interval * current_reward
        current_reward /= 2
    return total

print "Total BTC to ever be created:", max_money(), "Satoshis"
```

There is running of the script:

Another example.

*Running the max_money.py script*

$ python max_money.py
Total BTC to ever be created: 209999997690000 Satoshis

This diminishing and finite issuance generate a fixed monetary issuance that resists inflation. Unlike conventional currency, which can be produced in infinite numbers by a central federal government, Bitcoins cannot be inflated by printing. Instead with Bitcoins, the opposite happens. That is deflation, a consequence of a fixed and diminishing monetary issuance. Deflation is a phenomenon of value appreciation as a result of a mismatch in demand and supply. This push up the value of the currency and exchange rate.

**A De-Centralized Consensus**

Bitcoin does not have a central authority, but every node has a complete copy of a ledger that can be trusted as the authoritative record. Blockchains are not created by a central federal authority, but made independently, by each node in the network. In a way, every node in the network, based on information transmitted through the insecure network connections can come to the same conclusion and make a copy of the same public ledger as anyone else in the network.

Bitcoin consensus is not achieved explicitly. There is no fixed time for consensus or election. The consensus is as a result of asynchronous interaction between thousands of nodes which act independently and follow simple rules. The consensus is emergent, and this is Satoshi Nakamoto
main invention of the decentralized mechanism. The decentralized emergent consensus of Bitcoin is from the interaction of four processes that independently occur across the network.

1) Independent confirmation of every transaction, by each full node, relying on a full list of criteria.
2) Independent aggregation of the transactions to new blocks using mining nodes, accompanied with demo computations by way of a proof-of-work algorithm.
3) Independent confirmation of new blocks by each node and placed into a chain.
4) Independent selection, by each node, of the chain using the most cumulative computation demo through proof-of-work

**Independent Confirmation (Verification) Of Transaction.**

In the later chapters, you are going to find out how wallet software make transactions by gathering OTXO, providing the right unlocking scripts, and then making new outputs assigned for a new owner. The resultant transaction is then transmitted to the neighboring nodes in the network: and later propagated to the entire Bitcoin network.

Nevertheless, before the transactions are forwarded to neighbors, each Bitcoin node that receives a transaction will verify it first. This is to ensure that only valid transactions are transmitted in the network. Those that are invalid are discarded by the first node that encounters them.

Every transaction is verified by each node against a checklist of criteria:

- The transaction data structure and syntax must be correct.
- No list of either inputs or output should be empty.
- The size of the transaction is less than MAX_BLOCK_SIZE
- Every output value, and the total must be within the accepted range. (more than zero, less than 21 m.
- No inputs have N=-1, hash=0 (coinbase transaction not to be relayed)
- nLockTime is equal or less to INT_MAX
- The size of the transaction is equal or greater 100 bytes
- The signature operation limit is more than the number of signature operations
- The unlocking script (scriptSig) push only the numbers on the stack. Standard forms must match the locking script (scriptPubkey). This will reject the non standard transaction.
- Matching transaction in the block or in the main pool branch should exist.
- Every input rejects a transaction if the referenced output exists in another transaction.
- For every input, check the main branch and the transaction pool to look for the referenced output transaction. In the case where the output transaction is missing for output, this becomes an orphan transaction.
- For every output that the referenced output transaction is a coinbase output, must have COINBASE_MATURITY (100) confirmation at a minimum.
- If the sum of output values is greater than the sum of input values, reject it.
• If the transaction fee is too low to get into an empty block, reject it.
• Unlocking scripts for every input should validate the corresponding output locking scripts.

These conditions change over time. This independent verification of every transaction before propagation builds a pool of valid new transactions.

**Aggregation of Transactions into Blocks**

Once the transaction has been validated, Bitcoin node adds it to the transaction pool, or memory pool, a place where transactions wait until they are mined/included into the block. (A person, for example, Isaac can mine Bitcoin through ‘mining rig’ a specifically designed computer hardware system for mining Bitcoin. This dedicated mining hardware is connected to a server that runs a full bitcoin node, which in this case we can call it Isaac node. Although you can as well mine without a full node.) Isaac’s node proceeds by collecting, validating and relaying new transactions like other nodes. However, unlike other nodes, Isaac’s node will proceed by aggregating this transaction into a candidate block.

A girl by the name Ann wanted some Bitcoins, so she exchanged some cash for it. The transaction was created by Martin, which funded Ann’s wallet with about 0.20 BTC. Ann used her bitcoin to buy a mug of tea at Jane’s restaurant. Let’s now have a look at the blocks that are created when Ann bought a mug of tea from Jane’s coffee. Ann’s transaction will then be included in block X (299,516). Now let’s assume that this block is mined by Isaac’s mining systems and keenly follow Ann’s transaction as it turns out to be part of the new block.

Isaac’s mining node will maintain a local copy of blockchain, which will entail a long list of every block that has ever been created since 2009, the beginning of bitcoin system. When Ann purchases a mug of tea, Isaac’s node assembles a chain up to block Z (299,514). Isaac’s node is very keen to listen for every transaction, to try and mine a new block as well as listen to other blocks that are discovered by other nodes. As Isaac’s node is busy mining, it gets block Y (299,515) through the network of bitcoin. The arrival of this new block implies the end of a very tough competition for block Y (299,515) and the start of a new competition to create block X (299,516).

For the last ten minutes when the node from Isaac was busy hunting for a solution concerning block Y (299,515), it was also busy collecting other several transactions to prepare for the next block. Therefore, at the end of the ten minutes, it will have collected a number of transactions in
its memory pool. When it has received block $Y$ (277,315) and validated it, Isaac's node will check any transaction in the memory pool and delete all that was contained in block $Y$ (299,515). Any transaction that remains the memory pool and is not confirmed remain to be recorded in another block.

Isaac's node instantly constructs another empty block, block 299,316 candidates. The new block is known as candidate block since it's an invalid block since it doesn't contain authentic proof of work. The only way to make a block valid is if a miner successfully finds a solution to the algorithm of proof-of-work.

**Transaction Fees, Age, and Priority**

To be able to construct candidate block Isaac’s Bitcoin nodes choose transactions from the main memory pool, it does this by successfully applying a primacy metric to every transaction and add the utmost-priority transaction first. The prioritization of transactions is based on the age of UTXO which is spent in their respective inputs, thus allowing for high-valued and old inputs to be given priority over smaller and newer inputs. Transactions which are highly prioritized can be sent with no fees, in case the block has enough space.

The prioritization of the transaction is calculated as the total sum of the age and value of the inputs divided by the size of the transaction:

$$\text{Priority} = \frac{\text{Sum (Input Age * Value of input)}}{\text{Transaction Size}}$$

In this equation, the age of UTXO is the total number of block which have elapsed ever since UTXO had been recorded on the blockchain, evaluating the number of blocks ‘how deep’ is it into the blockchain, the value of input is measured in base unit, satoshis, which is 1/100m of a bitcoin. Transaction size is measured in bytes.

In order for any transaction gain the status of high-priority its priority should be greater than 57,600,000, which actually corresponds to 100m satoshis (1 bitcoin), one day old (144 blocks in number) in a transaction of about 250 bytes in size.

Therefore, $\text{High Priority} > \frac{100,000,000\text{satoshis} \times 144 \text{blocks}}{250 \text{bytes}} = 57,600,000$

However, the first fifty kilobytes of transaction space in a given block is set aside for highly prioritized transactions. Isaac's node would fill the 50 kilobytes first, prioritizing the highly prioritized transactions first, irrespective of the fee. Hence, allowing the highly prioritized transactions to be processed faster even if they do not carry any fee.

Isaac's mining node will then fill the remaining of the blocks up to the fullest of the block size (which can be expressed as MAX_BLOCK_SIZE in the code), where any transaction that carries the minimum fee will prioritize the ones that carry the highest fee per kilobyte.

If there is a space that has been left in the block, Isaac's mining node might prefer to fill it without any transaction fee. Some miners might decide to mine transactions with no fee on the best effort
basis. While on the other hand, other miners might decide to ignore any transaction that has no fees.

Any other transaction that is left in the memory pool, after the block has filled up, will just remain in the pool to be included in the next block. As a transaction remains in the memory pool, its input ‘age,’ as UTXO continue to get deeper into the blockchain as new blocks are added on the top. However, since the priority of a transaction depends on the age of their inputs, all transactions that remain in the pool will age, thereby making its priority to increase. Finally, all transactions without fee could reach maximum priority to be incorporated in the block for free.

Transactions of bitcoin don’t have some kind of expiration time-out. Any transaction which is valid right now will always be valid for eternity. However, if the transaction is spread across the network once it will continue so long as it’s held in a mining node memory pool. You should know that if mining node is restarted, then its memory pool is automatically cleared since it’s a transient non-continuous form of storage. Even though a valid transaction might be spread across the network, if it’s not executed at the right time it might eventually non-reside in the memory of a pool. It is expected that wallet software will retransmit such kind of transactions or even reconstruct them with much higher fees in case it is not effectively executed within a reasonable time frame.

When Isaac’s node aggregates each and every transaction from memory pool, newly formed candidate block with 419 transactions has about 0.09094923 bitcoin in transaction fees. This can be seen in the blockchain by the use of Bitcoin Core client command-line:

```bash
$ bitcoin-cli getblockhash 299516
0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4
$ bitcoin-cli getblock
0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4
```

A good example of this is as follows

```json
{
"hash": "0000000000000001b6b9a13b095e96db41c4a928b97ef2d944a9b31b2cc7bdc4",
"confirmations": 35561,
"time": 218629,
"height": 299516,
"version": 2,
"merkleroot": "c91c008c26e50763e9f548b82fc323735f73577effbc55502c51eb4cc7cf2e",
"tx": [
"d5eda064c617ca25ec1309bd160c3c1b77e1c0e6a2e73cda15c737e7424afba2e",
"b26bb45c55b39d759f147f7718b9918ca0ba3d97e56f3b91956fe977c503f6e",
... 417 more transactions
],
"time": 1388185914,
"nonce": 924591752,
"bits": "1f03a0c",
"difficulty": 1180923195.25802612,
"chainwork": "0000000000000000000000000000000000000000000000000934695e92aaf53af01",
"previousblockhash": "0000000000000002a77bd25a170c374cc55261021e8a9ca7442b0128f0569",
"nextblockhash": "00000000000000010236c269dd6ed714dd5db3936b33959079d7b8fd431ba7"
}
```
**Generation Transaction**

The initial transaction that is added to the newly formed block is a distinctive transaction, known as *generation transaction* or in some cases *coinbase transaction*. Isaac's node constructs this transaction, making it his reward for the effort of mining. The node ends up creating a generation to work as payment to Isaac's wallet: paying Isaac's address 25.0904923 bitcoin. This is because the sum amount of reward which Isaac collects for mining the block is the total of transaction fees (0.08094927) and the coinbase reward (25 new bitcoins) from every transaction that is included in the block.

![An example of this is as follows below.](attachment:image)

```
$ bitcoin-cli getrawtransaction
d5ada064c6417ca25c4308bd158c34b77e1c0eeca2a78cda16c737e7424afba2f 1
```

Generation transactions do not spend (consume) UTXO as inputs like regular transactions. As a matter of fact, it has one input only, known as coinbase; it works by creating bitcoin from nothing. Generation transactions have a single output, which is only payable to the address of bitcoin.
miner. The generation transaction's output sends 25.0904923 bitcoins to the address of bitcoin miner, which in this case it is 1MxTkeEP2PmHSMze5tUZ1hAV3YTKu2Gh1N.

**Coinbase Fees and Reward**

To create a generation transaction, Isaac's node calculates the sum of transaction fee first through the addition of all outputs and inputs of 419 transactions which were earlier added to the block. Total fees are workout as follows: \( \text{Fees} = \text{Sum (Inputs)} - \text{Sum (Outputs)} \)

In our earlier block 299,516, the total transaction fee is 0.0904923 bitcoin.

After, Isaac's node accurately calculates the right reward for the newly formed block. The calculation of reward is based on the height of the block, starting at fifty bitcoin/block and then reduced to half after every 210,000 blocks. Therefore, since our block is at 299,516, this means that our correct rewards are about 25 bitcoin.

This calculation is seen in the function `GetBlockValue` of the bitcoin core client. The example of calculating block reward, `main.cpp`, line 1305 is as follows.

```c
int64_t GetBlockValue(int nHeight, int64_t nFees)
{
    int64_t nSubsidy = 50 * COIN;
    int halvings = nHeight / Params().SubsidyHalvingInterval();

    // Force block reward to zero when right shift is undefined.
    if (halvings >= 64)
        return nFees;

    // Subsidy is cut in half every 210,000 blocks which will occur approximately every 4 years.
    nSubsidy >>= halvings;

    return nSubsidy + nFees;
}
```

The first subsidy is evaluated in satoshis by multiplying fifty with a constant COIN (100,000,000 satoshis). Thereby setting the first reward Subsidized to a 5.0 billion satoshis

**Successfully Mining the Block**

Since Isaac's node has constructed a candidate block, it's time Isaac's hardware mining rig to effectively mine the block, as well as finding the solution to the algorithm of proof-of-work, which makes the block to be valid. As we have seen and we will continue to see in this book, the hash function SHA-256 is one of the main function that is used for mining process of bitcoin. Isaac uses a lot of hardware mining rigs with ASIC (application specific integrated circuit). Here thousands of integrated circuits work the SHA-256 algorithm in parallel at a tremendous speed. The connection of these specialized machines is via a USB to his mining node. The mining node working on Isaac computer will next transmit the block header to his mining hardware, where it will start testing trillions of nonce per second.
After around 11 minutes immediately after starting mine, block 299,516, one mining machine hardware locate a solution and transmit it back to the mining node. Nonce 4,215,469,401 if put into the block header will generate a hash of 0000000000000002a7bbd25a417c0374cc55261021e8a9ca74442b01284f0569, which is < than the target of 0000000000000003A30C00000000000000000000000000000000000000.

Instantly, Jing mining node sends the block to all the peers. The peer nodes receive, validate and propagate this new block. While the block continues to be transmitted in the network, every node takes a copy and add it to its blockchain. As this miner receive, validate, and propagate the block, they forfeit their effort to find a block of the same height and instantly begin computing the adjacent block in the chain.

**Chapter 4: Should You Mine in a Pool or Solo**

Selecting the method to use during mining is important. Mining is mostly considered a chance activity and the probability of winning a block within a particular time. Many systems will require more time to get a good chance of mining a single block, and sometimes it can take months and even years. It is important to select a suitable method that miners use. The method needs to be
effective and easy to master with less complication. A suitable method of mining needs to be simple; this will give room for adjustments and manipulation of formulas.

The number of machines running at high hash rates is important in ensuring that one finds several blocks easily. The machines set will aid in absorbing the variation in the same rate at which the blocks are mined. When one decides to run a lower hash rate machines, one will need to run for longer periods hoping to get a block. Whatever the method selected, mining is regarded an expensive deal, and therefore, one has to work within their budgets. When one selects pool or solo mining, it is important to realize that machine maintenance is necessary at all times. When machines are constantly maintained, the hash rates tend to increase and chances of mining more blocks increases.

Developers and statisticians have come up with a formula that will help one find how much they can mine in a particular period. The formula is derived from the difficulty that one has and the hash rate of the machines they are using to mine blocks. When the formula is effectively applied, one will be able to find the duration it will take for a single block to be achieved.

Time=difficulty*232/hashrate

For the formula to generate effective results, it is important for one to apply the current difficulty, rather than using either days or months, issues to calculate the amount generated. The likelihood that one finds a block will depend on how you have compared total network hash rate to the current hash rate of the machines. One can also apply another formula derived from the hashrate

Hashrate=total network hashrate/144

The number 144 is replaceable by the number of blocks chain mined that particular day. The hashrate is the duration that it takes for a single block to be attained in the process. Let’s assume one is mining in a pool where one can earn fractions of blocks compared to the efforts, the formula required to calculate the total mined in a day is;

Hashrate=Total Network Hashrate/3600

The value 3600 is applicable because the average number of bitcoins expected in a day is within that value range. Given that there are six blocks per hour and the block reward is 25, we can calculate the following:

6 blocks/hour X 24 Hours per day X 25 BTC/block=3600 BTC/day

It is therefore important to understand the hashing power that one’s machine can generate, if the hashing power is high, one might consider mining solo. Where one has to wait for at least six months to earn a block, it is important to consider doing pool mine. This is important in the sense that after that period one will be able to get back their investment and with profit. Whatever method one decides, it is important to look carefully for the return attained, and whether one is
willing to wait for that duration to enjoy the outcomes. The other factor that one might need to use when selecting the method of mining is the risk encountered and how one is capable of handling the difficulties in a particular time.

The sharing of information on the best methods of mining is increasing, and thus the number of people willing to mine increases; this in return reduces the individual block mined in a given period. The upside to a larger network is that everyone using it becomes safer, the more people involved in mining, the lower the risk one may encounter because the network becomes more stable. The mining field has many good and bad intention individuals. Therefore, the higher number of users reduces the risk of attack because an attacker will have to use more effort to bring the system down. A larger network also allows a higher total transaction rate. The rate of the transaction is important in reducing the duration it will take to find a block, thus when many people have the information, and willing to invest in this lucrative business, they will mine more blocks in the end.

**How to solo mine**

Solo mining is the process of mining alone. When you solo mine you connect your miner to your local bitcoin client and try to find a block on your own. The probability of gaining any is very low, but sometimes it is very rewarding given how the bitcoin networks operate, in a very long period both solo and pool mining can receive the same amount of blocks. As I had mentioned earlier, in realistic timeframes though pooled mining is definitely the better way if you have hardware with the small hash rate.

Solo mining will start by running a personal copy of bitcoin-qt which is an address that one installed into their system, it helps one in the mining process. Bitcoin-qt will be the wallet where your received blocks will be stored. The software is downloadable since it is a free firmware and anyone can access it online.

**Step by step of setting up a solo mining server**

**Step 1**

Configure the startup script, which will be the start menu on windows on a personal desktop. Then include the line flag-server. When this is done, it will automatically turn on the RPC servers that allow direct communication with the miners.
Step 2

You will be required to edit the bitcoin.conf file, which will be located in the personal installation user’s directory. For Windows users, this will be located at `Users/Peter/AppData/Roaming/Bitcoin` directory. I used my name here; you will have to find from your personal computer and the user’s name for the process. Finding the app data can be sometimes difficult for those with little knowledge about computers. The first thing is to locate the local disk C, the on the option part, select show hidden files, the app data will be displayed among the folders. You can edit this file using the notepad, notepad++, Ultra edit or use any other tool that keeps the file in the text format. In the editing process, it is not advisable to use the WordPad or the Microsoft words as they will convert the format to a format other than raw text which the Bitcoin-QT will fail to recognize it.

If you don’t have a bitcoin.conf file, then you will need to create one. There are so many online sources that allow people to create one; a good example is of the bitcoin.conf can be found in https://en.bitcoin.it/wiki/Running_Bitcoin#Sample_Bitcoin.conf

Put the following lines in the bitcoin.conf:

```
server=1
rpcuser=username
rpcpassword=password
rpcallowip=127.0.0.1
rpcport=8332
```
Then use 127.0.0.1:8332 as the server and the username and the password you choose as the credentials to connect BFGminer or CGMiner to the Bitcoin_core client and have it mine.

If you are going to mine from another computer, meaning you are not running the client software on this same computer, you will also need to configure the following parameter.

```
rpcallowip=192.168.1.110
```

The IP Address should be the IP address of the computer running your miner. When you are mining it is very important to make sure that your computer is not using DHCP. This is important because when there is a change in the IP address, the mining process will stop until you notice there was a problem and thus gives one an opportunity to change.

**Step 3**

Restart the server. That is all that you will need to set a solo mining server.

Solo mining for profit is not possible. There are a fixed number of bitcoins released when applying such a method. This is due to the number of many people fighting for the same source of bitcoin; the miners get less and less in the end. Therefore, if one wishes to mine for profit making, the duration it will take them to release the profits or investment is very long. The complication in gaining the blocks is thus the main reason one can take ages before a reward is obtained on average.

**Advantages of solo mining**

High variance - when using solo mining one can easily mine 25 BTC once in a year, and with the increase in the value of the currency, one can be lucky to get few extra bucks annually. Sometimes with some bad luck, the number mined can be below 15. If one has a fast hash power, maybe you receive payments every month or on average six weeks.

No fees: setting up a solo mining is easy and no extra charges that one may incur. It is the best earning if you do merge mining and do the work to ensure that the orphan rates are low. Despite not merging being an advantage, it sometimes reduces the total earning to negative, where one will make less than you would have at a low-fee merged mining pool.

High trust: When one has a little technical skill, it is easy to trust yourself, it is also easy to monitor the process by yourself as it runs and in case of issues, you can easily adjust and make it better.

**Disadvantages of Solo mining**

Complicated setup: You will want to do merged mining otherwise you make much less than in a merged mining pool. Sometimes the publically available pool software is outdated, broken, inefficient, and no longer maintained in many cases. For you to ensure there is no orphaned block you need good connectivity to the bitcoin peer-to-peer network.
Solo mining requires a lot of his power and is not for the faint-hearted. It will require a lot of time before one realizes any profits and investment values. Many have questioned the benefits derived from solo mining; sometimes the risk involved is not worth taking.

**Pool mining**

Many are taking part in the cryptocurrency mining, and it is not surprising to find some pools running at any given time. When deciding to pool mine, there are some things to consider. There is a balance. The larger the pool, the smaller the pool fees which will be required to manage such a particular pool. The larger pools tend to spread risk to many miners, thus regarded as more price sensitive. Different miners will have to share the cost of the service; it is advisable to go for the one where the number of miners is higher. The advantage is huge, and the risk of hacking is very low, as I had mentioned earlier. However, as a community, we do not want any one entity to manage 51% of the entire network hash. When an entity has a huge percentage, it is easy to allow a high attack on the entire system.

When the attacker controls, more than 50% of the network computing power, in many cases they control and modify the ordering of transactions. This will give him/her an opportunity to reverse transactions that he sends while in total control. This will have the potential of double spend transactions that was previously located in the blockchain.

Attackers who control more than 50% can also prevent some or at times all transaction from gaining any confirmations. This is risky because they will hinder others from accessing their mined coins. The attackers also have the advantage to prevent other miners from mining any valid blocks. These are some of the reasons; one operator cannot control more than 50% of the entire mining system pools. The process of mining being online encounters challenges from hijackers and even with less than 50% control, many attempts to change the system with 100% fails.

When using pool mining, it is easy to attain 50BTC for 95% of the time, and it has always been a success. Sometimes miners prefer one pool to another due to the slight difference in them. There are some factors such as:

- Do they pay transaction fees into the pool?
- What is the pool fee needed?
- What is the payout system, this can be the reward attained in the mining?
- Can you withdraw your funds immediately? Alternatively, do you have to wait for 24 hours before the request is granted?

**Payout systems**

There are some payout systems. I will explain the details of each system:
Double Geometric Method (DGM)-This is a hybrid between the PPLNS and geometric reward; types that enable the operator to absorb some of the variable risks. The operator thus receives a portion of payout on short rounds and returns it on a longer rounds to equalize the payments. It is the course of hopping proof, the expected payout per share is always the same no matter when it was generated. In most cases, the variance and the maturity time (the time it takes to receive the reward) are totally independent of the pool's history and completely independent of the future difficulty changes.

The method is purely score-based, which means that all the information required to calculate payout can be encoded with a single score value per participant. In this case, there is no need to keep the history of the shares. However, it is advisable to use a logarithmic scale to store their values and do the calculations; this is because the score grows exponentially.

I will denote by B the block reward (assumed constant) and p = 1/Difficulty. Also, there are three parameters which can be adjusted to balance average fee, operator variance, share- and pool-based participant variance, and maturity time:

- f - Fixed fee.
- C - Average variable fee. The average total fee will be (c+f-cf)B per block. Increasing c reduces participants' variance but increases operator's variance.
- o - Cross-round leakage. Increasing o reduces participants' share-based variance but increases maturity time. When o=0 this becomes the geometric method. When o->1 this becomes a variant of PPLNS, with exponential decay instead of 0-1 cutoff (note that "exponential" does not mean "rapid," the decay can be chosen to be slow). For o=1, c must be 0 and r (defined below) can be chosen freely instead of being given by a formula.

**The method is as follows:**
1. When the pool first starts running, initialize s=1. Initialize the scores of all workers to 0.
2. Set \( r = 1 + p(1-c)(1-o)/c \). If at any point the difficulty changes, p and then r should be recalculated.
3. When a share is found, increase by p*s*B the score of the participants who found it. Set s=s*r.
4. If the share found happens to be a valid block, then after doing #3, also do the following for each participant: Letting S be his score, give him a payout of \( (S(r-1)(1-f))/(ps) \). Set S=S*o. The remaining reward is given to the operator. Or, if the total is higher than the block reward (only possible if f<0), the operator pays the difference out of his funds.

The intuition is this: Instead of keeping the score unchanged when a block is found (as in PPLNS) or setting all scores to 0 and effectively transferring them to the operator (as in the geometric method), a part of the score is transferred to the operator. When rounds are long, participants get to keep most of their score between rounds and this is similar to PPLNS. However, if several blocks are found in rapid succession, the operator will collect a large portion of the score and thus be the primary beneficiary of the good fortune. The fees collected this way allow letting f
be negative, sweetening the rewards of long rounds. Overall, this decreases the dependence of participants’ rewards on the pool’s luck, thus reducing the variance caused by it.

The variance of the payout for a single submitted share is

\[(1-c)^4(1-o)(1-p)p^2(1-f)^2B^2 \]

\[\frac{1}{(2-c+o)c+(1-c)^2(1-o)p}\]

**Proportional (Prop)**—When block is found the reward will be distributed among all workers proportionally to how much shares each of them found. When you submit a share to a pool, there are only two categories, under the current difficulty, and over the current difficulty. When doing the proportional, a share submitted having a higher difficulty could still count the same as a share submitted having low difficulty. This is to say that the only time a pool cares about the submitted difficulty is when it’s over the network difficulty, and it counts as a block solve.

**Pay Per Last N Shares (PPLNS)**—Many as being similar to that of proportional describe this. The difference between the two, proportional looks in details about the number of shares while this will only major on the last N shares, regardless of the round boundaries.

**Pay Per Share (PPS)**—Its value share is worth certain amount of BTC. When calculating the blockchain using the method, the block will require current difficulty and shares on average. The PPS method will have 0% fee and can generate 25BTC; this can then be divided by the current difficulty. The only disadvantage with the method is because it carries with it high fee charges.

**Shared Maximum Pay Per Share (SMPPS)**—This is similar to pay per share, but the difference is that it does not pay more than the pools earn. Meaning every member will receive the payment for every share generated, but no one can have more than what the pool earns. The value is shared equally among all the users.

**Equalized Shared Maximum Pay Per Share (ESMPPS)**—This is similar to the SMPPS, but the difference arises where the system allows the owners to receive a much higher pay compared to other members. Therefore, the payments are equalized among all those who owed it.

**RECENT SHARED MAXIMUM PAY PER SHARE (RSMPPS)**—The systems works similar to the SMPPS, but it gives priorities to the most recent miners. The recent miners are paid their due, and then the existing miners share the rest. This is good because all members receive depending on the duration they have adopted the system.

**Pay On Target (POT)**—The system is designed in a way that reward is awarded based on the level of difficulty. The high variance PPS variant that pays on return to the pool rather than the difficulty of work served by the pool.
**Score based system** – this works similar to the proportional reward system, but the difference arises where the reward is weighed by the time it was submitted. Each submitted share is worth more in the function of time t since the start of the current round. For every share, score is updated by: score += exp(t/C0. This in return makes the shares worth much more than earlier shares, therefore, the miners score quickly diminishes when they stop mining on the pool. In pool mining, the hash rate is largely irrelevant since it is not a popularity measurement.

**Characteristics of pool mining**

The calculation is mostly theoretical; this shows how the system is complicated and thus good for security and maintenance. This makes it important in ensuring that no single pool gains control of more than 50% of the total computational power of the network.

The merged mining allows miners to mine on the multiple block chains at the same time with the same hashing power. This unique feature makes the system more powerful compared to that of solo mining that requires more hashing power and only generates few blocks chain after a long time.

3.0, 3.1, 3.2, 3.3, this pool is effective in rewarding user’s stale shares.

4.0, 4.1, 4.2, 4.3, 4.4, 4.5, 4.6, 4.7, 4.8 these will allow the difficult part of the shares to be changed by the users when they are operating in the system, thus making the mining procedure easy and smooth.

5.0, 5.1, 5.2 this allows the miners to operate the proxy available

When the mining is merged, it is easy for one to operate a solo mining basing on the payouts that have been joined by the merged chain from the pool.

An individual known as the pool operator runs mining pool. This pool operator will act as the recipient of all block rewards for blocks found. The operator will also be responsible for paying all the miners in that one particular pool. There have been two main dominant rewards types that are a double geometric method, which has been explained partly on this book and Pay Per Share PPS. With the use of PPS, one will know exactly how much you will earn from each hash regardless of the blockchain found. The system allows users to move the money as soon as they receive it. This is the best style that you need to apply as a miner to enjoy the reward as soon as earned.

Many miners have agreed that DGM, double geometric method is the best reward system out there. The good results can be experienced if you stick with the system for long. As a test, I operated two pools with different reward types. To compare the two, I used a two-week period with the same level of difficulty. The first week I used the DGM and the second week I used the PPS. The PPS recorded more results. The DGM does not pay on blocks until there are 120 confirmations, which only happens after 24 hours. The double geometric method has an
advantage to the operator since the risk is reduced as compared to PPS. In PPS if the pool operator does not earn enough from the foundation blocks to repay the miners, the operator has to come up with extra Bitcoins, this will not happen in the case of DGM.

**Using a pool**

After picking a pool to use, you will need to set up an account and configure your miner to log into the pool. The pool consists of two interfaces. The first interface is the one that the mining software uses to get work and report the finding results of the work done. The second interface allows you, the user, and the ability to interact with the system. In this part, I will review two mining pools. The most popular mining pool is the BTC guild, and the other is the 50BTC. I will share the information about the site and the registration procedure.

**50 BTC**

This is named after the amount of reward that is found block in the first four years. 50 BTC has the lowest PPS rates, which in many times ranges between 2.5% and 3 %. They do not pay transaction fees but tend to have the unreliable infrastructure, a responsive support portal, and payouts occur faster. The website address link is [https://50btc.com/](https://50btc.com/)

The main account page provides you with the current balance, a history of your mining effort, history of the difficulty, along with a calculator that can be used to translate a given hash rate amount into BTC per day or USD per day. The calculator is very handy, hence the handy name dandy. The mining provides you with stats for your mining history. The other feature is the payout,
which allows you to pay in many different ways including liberty reserve among other many methods. The payout page will show the history exception of one time; it takes an average of one minute to receive the payout when the transaction is transmitted. The good thing about the account is that it is easy to track the transaction even where your account was hacked.

For you to receive BTC, click the payout button and enter the amount of BTC YOU WANT SEND TO YOUR address. The first thing to do is always to send the Bitcoins to your wallet before taking another transaction to someone else. This is important in case one returns the bitcoin, they will not accidentally payback to the pool address, when such a mistake happens the send coins get lost. The good thing about 50BTC is that it has its default to using HTTPS, this is not the case on the BTC Guild. The 50BTC is 3% and is joined, whereas BTC Guild is 5%.

**BTC GUILD**

The system has a well-put-together user experience. On their website, the how to mine part explains where to get the software and what details are required for configuring the miner. The site also provides a clear explanation of how they pay out, for both the PPS and PPLNS (Pay Per Last N Shares). Many people have joined the site and tried to mine; this provides much easier mining efforts.

In the news section, it is refreshing to see that the site has implemented a 51% mitigation plan to reduce the likelihood that they would reach 51% of the network. In essence, they are going to keep raising the fee until people leave; this then reduces the fees once the levels are low enough that the community is not fearful of the pool obtaining 51% of the network.

There are tabs that detail each worker, payment stars, ranking and pools stats. The user interface is easy to navigate and looks nicely polished.
Chapter 5: How To Set Up A Bitcoin Miner

Setting up a Bitcoin miner and starting to generate Bitcoin is just simple. All you require is the right tools and knowledge on how to go about it. Therefore, you need to apply some effort and spend some time in getting all the information you need to avoid making mistakes that may eventually discourage you from getting to mine. Below are the best steps that will guide you to set up a Bitcoin miner with less struggle and little effort.
Step 1. Purchasing a Custom Mining Hardware

Before purchasing a mining hardware, it is important to have a full understanding of what mining is and how Bitcoin mining works. This theory basis forms the right basis for you to easily get into the practical part of starting to mine, and generating as much digital cash as you have ever wished. The next key factor is deciding on the most suitable hardware to purchase. Therefore, before you purchase any hardware and get to start mining, you need to consider certain hardware properties in order to go for the best. These properties include

**Hash rate.**

The strength of any mining hardware is determined by the number of calculations within a second that it can make. Therefore hash rate is referred as the calculations hardware performs in every second, when making computations to solve the problem presented by the mining section. Hardware with the highest hash rate ability is ranked the best when it comes to solving any sort of a transaction block. To determine the best hash rate, a miner will have to compare their hardware hash rate with the average current hash rate. To learn more about on hardware hash rate, you can contact this site. [bitcoin wiki’s mining hardware comparison](#)

**Energy consumption**

The earlier Bitcoin pioneers mined Bitcoins using GPU and the CPU in their desktops or the video processor cards with very high speed. Today, the same could be used, but the impacts of the returns make it unbearable hence making it impractical. Currently, there is the most preferred customized Bitcoin mining. This is the ASIC chips customized Bitcoin miner. This systems’ speed is hundred times faster compared to the older systems speed. No wonder it has dominated the entire industry of Bitcoin mining.

Determine the number of hashes you are likely to get from each electricity watt consumed. This is calculated by dividing the hash produced with the electricity watts consumed. For instance, if the hash rate for your device is 500GH/sec and it utilizes an electric power of 400 watts, then you will get 1.25 Gh/sec for every watt used. By use of an online electricity price calculator, you will be able to change this to hard cash and realize the total electric power bill you have spent.

Well, you will realize that some hardware may consume electricity at a very high rate, making you spend on it than you can really earn from mining the Bitcoins. Moreover, using your mining system for other activities lowers its speed, and increases the electricity usage hence high electricity bills. Therefore, you should choose the best hardware for Bitcoin mining which is built for only mining purpose. Such companies as the Avalon will perfectly build a specific Bitcoin mining hardware for you.

**Why custom hardware is the best**

- Custom hardware has a better and faster processing speed.
• Custom hardware has a similar look like a graphics card. It is therefore easily inserted into your device; laptop, smartphone or a desktop as soon as you plug them into a power source.
• Bitcoin mining hardware is widely available. Among the most common brands for Bitcoin mining include; Coin Terra, Bitcoin Ultra, and the Butterfly Labs.
• There are a variety of Bitcoin mining machines that are affordable to everyone. Their cost ranges from ten thousand dollars to hundred dollars depending on their hash rate; calculation completed in every second.

Categories of Bitcoin Mining Hardware
The three major categories of Bitcoin mining hardware are; the ASICs, the GPUs, and the FPGAs. These are discussed below.

GPU/ CPU Bitcoin mining
This kind of hardware was used in the olden days when Bitcoin mining was introduced. It can be used even today. However, being the least powerful, with slow processing speed makes it unable to meet the current standards of hardware in the Bitcoin mining industry. However, in case it is the only device you can use, there is a way of boosting its speed, this is through adding a graphics hardware to your device. A graphical card contains features of a graphical processing unit (GPUs), mostly used in video games using the high-end cards. They have an added mathematical lifting power, which makes them perfect for carrying out hash rate computations necessary in solving transaction blocks. To purchase the graphical processing unit, you will find them in Nvidia and the ATI vendors.

Though the high-end graphical cards are quite expensive, costing about $100+, their speed is much better compared to CPU hashing. For instance, the CPU will give a hash of 10MH/sec, while ATI5970 gives a hash of 800MH/sec. Additionally, the GPUs, is open to being used by other miner options in the cryptocurrency industry, such that you can use them to mine Bitcoin as well as in mining Litecoin among other coins. Unfortunately, the introduction of the ASIC mining hardware has rendered GPUs extinct in Bitcoin miners industry. This is because the GPUs power cannot offer any competition with the ASIC, as its speed is miles ahead.

FPGA Bitcoin Mining
FPGA means a Field Programmable Gate Array Bitcoin mining hardware, designed in such a way that it requires to be built first, and then configured into the system. The hardware manufacturer, therefore, purchases many chips, then they are customized for mining of Bitcoins, after which they are put into various devices. Being mining customized makes them best miners over the GPUs and the CPUs. One chip of FPGAs can, therefore, produce an estimation of 750MH/sec. Besides one can put two-three chips in one box.

ASIC Bitcoin Miners
ASIC Bitcoin miner is the best Bitcoin mining hardware ever known. It is an integrated circuit, designed to carry out a specific activity; Bitcoin mining. The Application Specific Integrated Circuit operates at a very high speed and consumes relatively low electric power. ASCIs will only allow the use of specific Bitcoin mining hardware or any other hardware for SHA-256 crypto coin. Today, many Bitcoin miners are manufacturing ASIC miners and chips for their own use. Being a single task circuit has enabled the ASIC to be at the top of the CPU, FPGAs, and the GPU regarding high transaction processing speed among other benefits.

ASIC Bitcoin miner may consume more time to produce, and they are much expensive compared to other miners. However, their speed is stunning and thousand times better. At the moment, the selling ASICs have a speed ranging between 5-500 GH/sec. Moreover, vendors are guaranteeing ASICs with power ranging around 2 terahashes/sec.

Bitmain AntMiner S9 is the top bitcoin miner in the market today. It is made up of 189 ASICs chips, with an hash rate of 12-14 th/s, which is equivalent to 1000,000,000MH. Remember the CPU can only operate within a few MH unless a graphical card is integrated.

Setting up a Bitmain AntMiner S9

The Bitmain AntMiner S9 operates with about 1275 watts. It is advisable therefore to plug it to two PSUs with 110v each for powering the miner. This may be a PSU with 650 watts and 1000 watts Gold rated PSU. On the hand, you could decide to use a power source with 220v so long it is able to distribute power units as required. PSUs designed specifically for Bitcoin mining can be used or even those designed for servers.

Setting up The Bitmain AntMiner S9

I. Using PCIe cable in your PSU connections, connect PSU to Bitmain AntMiner S9.
II. Then after connecting the miner, you are required to connect cable; Ethernet directly to the miner.
III. Turn on the power system unit to power the miner.
IV. Enter an IP address to any device; smart mobile phone or a computer that is sharing the same network with the miner. Most miners today are DHCP enabled hence you will see your IP address on the router of your device, or you can use a scanning tool such as the AngryIP to scan any device connected to your network, including the antMiner IP address.
V. Then type the AntMiner IP address in the window of your browsing device.
VI. Feed in the login details to the first screen appearing in order to get to the miner. For the S9 miner, the word “root” is used both as a username and a password.
VII. A system overview appears on your window screen, first of all, change your password by clicking on the admin tab and add a password of your choice for security reasons.
VIII. Get to the tab on miner configuration and add your mining pool information. i.e. is your mining pool IP address, your worker name as well as its password. You can use “1234” as
the password for your mining pool since most pools do not need any password.

IX. Start mining as soon as your miner settings have been saved. For the hash rate to fully appear on the mining pool.

X. Get to the page on miner status, check on whether there is connectivity, check the hash rate, temps as well the miner performance. On checking the status of your Bitcoin mining pool, it should indicate that “you are mining Bitcoin now.”

Note that an AntiMiner has a forum page where the miners can discuss on various issues concerning mining.
Step 2. Obtaining a Bitcoin Wallet

A Bitcoin user wallet is a digitally encrypted wallet, necessary for every user to ensure the safety of their Bitcoins. There are both online and local Bitcoin wallets depending on what a user will prefer. However, most users will prefer using the local wallets; simply because no one could access them in case, any cryptography problem occurred.

The most common wallets in the industry of Bitcoin and other crypto coins mining industry include the following; Armory, BitcoinQT (Bitcoin Core), Multibit, Bitcoin Knots, BitGo, Bither, Electrum, Green Address, mSIGNA and the ArcBit.

Armory

This is an advanced local wallet Bitcoin client with features that allow the use of Bitcoin power by the users. With this wallet, you can be sure of strong backup in case a problem occurred. It has encryption features that enhance security and allow cold storage of your coins even when your device is offline.

BitcoinQT (Bitcoin Core)

Bitcoin core is a full local user wallet forming the backbone for Bitcoin network. It is, therefore, able to offer a high level of security, stability, and privacy. However, its usability is limited by the fewer features that make it to occupy large memory and space of the system.

ArcBit.

Its design is very easy and simple to understand and use. With the ArcBit user wallet, a user can be able to control their Bitcoins fully. Besides, it has an optional feature that of cold storage whereby the user can authorize payments even when their device is offline and are sure of enhanced security.

Bitcoin Knots

It has similar features as the Bitcoin Core; full Bitcoin client, that build the Bitcoin network backbone. However, though not tested well as the Bitcoin Core, their features are well advanced.

BitGo

This is a highly secured user wallet with a multi-sig. Hence the Bitcoin is free from loss and theft when using it. They offer full custody of your coins since they cannot freeze or spend your funds. Having features of security, they limit spending and any access by the multi-users. Additionally, BitGo wallets are simple and easier to use.

Bither

Bither wallet has an open feature enabling it to be used on various platforms. It is designed to have special features such as hot and cold modes with enhanced simplicity and high level of
security. To access different sources and generate a random number that is true for every user, Bither’s XRANDOM is used. HDM could also be used for multi-sig security and HD’s advantages.

**Electrum**

This is a user wallet with high-speed levels, enhanced simplicity, and low power usage. It is much suitable for handling most difficulty and Bitcoin system’s complicated parts. It has an added advantage of recovering your wallet’s secret phase.

**GreenAddress**

With a multi-sig and a user-friendly wallet that helps keep your keys highly secured and private. It uses an android app, browser extension, and 2FA to enhance security.

**mSIGNA**

This is a highly advanced, faster and easy to use wallet. It has a strong security and a high level of enterprise scalability. Its advanced features enable, paper backups, multi-device synchronization, electronic encryption, supports the multi-signature transaction, BIP32, and offline storage.

It is important to note the following advantages of using a local wallet;

- They are more secure, hence they are used by most Bitcoin users who are well established in the mining industry
- Local wallets require verification of the transaction blockchain hence keeping Bitcoin running and well secured

**Step 3. Secure Your Wallet**

Securing your wallet means that your wallet is free from loss and theft. You should, therefore, ensure that it is impossible for any unauthorized user to transfer your money by having full control of your security and privacy. However, Bitcoin guarantees full security and privacy to the user as long as their conditions are well observed. Additionally, it is important to be wise when using online wallets. There has been an online security breach before and till today; there is no high-
level security or insurance in case of loss like the banks do. Moreover, whichever, the kind of wallet you use, it is important to have a two-factor authentication.

Tips on how to secure your wallet

i. Just like with the banks, always keep small Bitcoin amounts in your server, computer or mobile phone for daily use. The rest you keep in more secured place

ii. Backup your wallet to protect you in case a computer problem happened. Backup also plays a crucial role in helping you recover your encrypted user wallet when your computer or mobile is stolen. To be safe and secure;

   **Ensure you back up the entire wallet**

   This will help you to recover your full saved funds even if some keys of your wallet are internally hidden. Otherwise, if you only have private key for the visible address of your bitcoin only, then some funds may be lost

   **Encrypt your online backups**

   Any backup that is network connected should be encrypted to avoid any losses resulting from malicious software and vulnerability to theft.

   **Use more than one secured locations**

   For security purposes, most people will use different media alternatives such as the CDs, USB keys, and the papers. A loss occurring in one location may not affect the rest, and more so, the recovery process will be easier.

   **Backup regularly**

   Soon, there is an invention that will require users to back up their wallet once, and their address changes are automatically updated. However, it is important to regularly backup your wallet regularly at the moment to ensure that any Bitcoin address created and recent Bitcoin address changes are saved.

   iii. Encrypt your wallet to ensure that you can set a password for any user withdrawing funds. To ensure that you have totally safeguarded your funds; you should remember your password always. Save it on a vault or a paper else you may permanently lose your funds. Use a strong password; at least with more than 16 characters containing numbers, letters, and punctuation marks.

   iv. Use offline wallets such as the cold stores for your Bitcoin savings. Any wallet that is not connected to the network provides high-security levels and is not prone to any computer vulnerabilities such as malicious software
v. Always update your software to be at per with the latest versions. This will boost security and stability of your Bitcoin software. New versions have new automated features for the safety of your wallet to provide a safe environment for your Bitcoins.

vi. Use Multi-signature wallets for theft and lose protection by enhancing approval of multiple independent spending. Most multi-signature wallets use a single server.

**Step 4. Decide the mining pool to join or whether to mine alone**

You could start Bitcoin mining as an independent miner, or you can join a group (pool) of miners to combine efforts and mine together. In case you join a pool, you will be able to share mining resources as well as split rewards for a Bitcoin created depending on the level of effort contribution during mining.

To mine alone if faced with a big challenge of high competition though when you make it create a Bitcoin you will enjoy the full reward. Nevertheless, this might takes you decades while pool mining yields quicker returns. Apart from reward sharing, most pools take 2% of the reward earned as pool charges. Create a worker immediately you join a pool to ensure that it keeps a record of the contribution you make when mining.

**Step 5. Download a mining program**

Various Bitcoin mining programs are open and free. You are therefore required to download a mining program that suits the special specifications of your computer. The most common mining software that is used in large scale today are;

- CGminer Bitcoin mining software
- BFGminer Bitcoin mining software

They are most preferred as they are designed to have a line of command program.

**CGminer bitcoin mining software**

This is the most common and famous mining software in the Bitcoin mining industry today. The miner is designed based on the code of the CPU original Miner. Its main features include; multi- sign GPU support, a CPU mining support, high speed with a fan control, a mini database offering new block self-detection as well as capabilities of a remote interface.

**BFGminer Bitcoin mining software**
BGFMiner and the CGMiner are almost similar. The only major distinguishing factor is that BGFMiner is specifically designed in line with the ASICs commands. On the other hand, the CGMiner focuses mainly on the GPUs. The major unique features of the BFGMiner are as follows; mining is done by use of a free LLVM OpenCL also known as mesa, uses a fan control speed with an integrated overclocking and an ID of a PCI bus with a reordering ADL device.

**Other common Bitcoin Mining Software**

**EasyMiner**

Easy miner is used to wrap up the BGFMiner and the CGMiner software conveniently. Its function focuses on GUI software. For stratum mining protocol and the protocol for network mining, the EasyMiner software is the best. The program works well for both pool and solo mining. EasyMiner software will configure your mining system and provide graphs for your performance to help you visualize the mining activity easily. Visit this page for the rest of the Bitcoin Mining software.

**Step 6. Run your miner**

The next thing after ensuring that your miner is configured is to start mining. You could do so by running a created batch line and waiting for the miner to connect after which you can start mining. When the miner connects, and the mining starts computer operating system assumes a crawling speed which is normal and expected.

**Step 7. Keep an eye on temperatures**

Mining activities and programs work hard on the hardware pushing them beyond their operating limits. This will mostly happen in case the hardware being used is used for other activities or its design was not meant for mining. A speed control fan program can help you to cool down the system when the temperatures are high and adjust them to be within the safe limits. Note that, when using the graphic cards, temperatures should be maintained at 80°C or below.

**Step 8. Check your profitability.**

To check on the profit you have earned is important, as it’s a measure that enable you determine whether you are earning or making losses, and whether Bitcoin mining is a worthy business for you. For excellent calculations, you are required to have a Bitcoin mining calculator and a profitability calculator. These assist in calculating the Bitcoin mining profit earned. Feed the following information to your calculator; the hash rate of your Bitcoin mining hardware in GH/s alongside consumed power in watts and the electricity cost in dollars per Kilowatt.
After that, the bitcoin difficulty, bitcoin price and the reward of a bitcoin block is featured automatically. This site provides further details in bitcoin mining calculator and profitability calculators.
Chapter 6: Top 6 Coins you can mine
Apart from Bitcoin

Mining cryptocurrency coins is an arms race which rewards quick adopters. Bitcoin has not only been a trendsetter, ushering in the wave of cryptocurrency that is built on a decentralized network of peer-to-peer; it has become de facto standard in the cryptocurrency industry. Other currencies which are inspired by Bitcoin are collectively known as Altcoins and have really tried to present themselves as improved or modified version of Bitcoin. Even though most of these currencies are simple and easier to mine compared to Bitcoin, there are several tradeoffs like bigger risk brought on by lesser retention, value, and acceptance. In this eBook we will focus mainly on six main altcoins, selected from over 700, though not in any specific order.

Ethereum (ETH)
It was launched in 2015; it is a decentralized software platform which allows Distributed Applications (ĐApps) and Smart Contracts to be built and run without any interference, fraud, downtime or control from a third party. In 2014, Ethereum launched a pre-sale for ether which actually received an overwhelming response. Ether, a platform-specific cryptographic token is the applications that Ethereum are run on.
Therefore, we can be able to say that ether is like a vehicle that moves around on Ethereum platform, which is sought by different developers who are looking to run and develop applications inside Ethereum. As a matter of fact, according to Ethereum, it can as well be used to “decentralize, codify, trade and secure about anything.” Due to the attack in 2006 on the DAO, Ethereum split into Ethereum Classic (ETC) and Ethereum (ETH). The market capitalization of Ethereum (ETH) is $4.4 billion, which is second after Bitcoin among other cryptocurrencies.

The biggest project Ethereum (ETH) has seen of late is the partnership between Microsoft with ConsenSys that offers EBaaS (Ethereum Blockchain as a Service) on Microsoft Azure in that Enterprise developers and clients can have a single click cloud-based blockchain developer environment. In 2017, ETH made a very big move when it established the Enterprise Ethereum Alliance that focused on promoting and building the best standards and practices to effectively facilitate the adoption of Ethereum procedure for the enterprise. Some of the greatest brands from insurance, consultancy, technology, and banking are part of Enterprise Ethereum.

**Litecoin (LTC)**

Launched in 2011, Litecoin was among the first cryptocurrencies following Bitcoin and was mostly referred by most people as “silver to Bitcoins gold.” Charlie Lee who was a former Google engineer and MIT graduate created it.

Litecoin is majorly built on an open source world payment network which isn’t controlled by any authority and uses "scrypt" like a proof of work that could be recorded with the assistance of CPUs of customer grade. Therefore, making it a well decentralized open source. As it can be seen Litecoin was built with an objective of improving the shortcomings of Bitcoins and over the years it has earned the support of the industry along with high liquidity and trade volume. It have a quicker block generation rate, thereby offering faster transaction confirmation. Apart from developers, there is a high growing number of merchants who accept it.

Litecoin is created to be able to produce more coins, about four times than Bitcoin, and at a faster rate of about a quarter of Bitcoin’s time. Generally, Litecoin has been seen as 2nd to Bitcoins in terms of value, although Litecoins are more easily transactional and obtainable.

**Zcash (ZEC)**

Zcash is an open-source and decentralized cryptocurrency, which was launched in latter part of 2016, and it looks very promising. For example, if HTTP in Bitcoin is for money, then https is Zcash; this is how Zcash defines themselves. It offers selective transparency and privacy of transactions. Just like https, Zcash has seen to claim that they provide extra privacy or security where every transaction is published and recorded on the blockchain, but other details like amount, recipient, and sender remain private.

The users of Zcash are offered a choice of ‘shielded transactions’ that allow all content to be encrypted through the use of the advanced cryptographic method or a zk-SNARK a zero-knowledge proof contraction developed by the team of Zcash.
In other words of Zcash is a new cryptocurrency and blockchain that allows private transactions or generally private information in a public blockchain. It allows new apps, consumer, and businesses to control who should see the details of one’s transactions, even when they are using a global, un-permission blockchain.

**Monero (XMR)**
This is said to be an untraceable, private and secure currency. Monero is an open-source cryptocurrency, which was launched in 2014 and it spiked impressive interest among the cryptography enthusiasts and community. Development of Monero cryptocurrency is totally community-driven and donation-based. This cryptocurrency was launched with a strong emphasis on scalability and decentralization, and it allows complete privacy through the usage of a special technique known as “ring signatures.” Availability of this technique, it looks like a group of cryptographic signatures that includes at least one actual participant, however since all of them appear valid, the real one can’t be isolated.

Individuals transacting in Monero could change it back to dollars or to either Bitcoin via a number of online cryptocurrency exchanges. The complete opacity and anonymity is something good, although it is also bad as black market denizens value it; though is frowned upon by law enforcement and regulators. If the usage of Monero is perceived to be of questionable activity or illegal, then its widespread use can be dampened.

**Ripple (XRP)**
This is a real-time global settlement network which offers low-cost, certain and instant international payments. Ripple (XRP) “enables commercial banks to settle their cross-border payments faster and in real time, at lower costs, and with end-to-end transparency.” Ripple currency was released in 2012, and it has $1.26 billion market capitalization. The consensus ledger of Ripple -- its conformation method – does not need mining, thereby reducing network latency and minimizes the use of computing power. Ripple mainly believes that ‘distribution value is a powerful method to incentivize specific behaviors’. Hence it is currently planning to distribute XRP mainly “through enterprise development deals, incentives to liquidity providers who propose tighter spreads for payments, as well as selling XRP to institutional buyers interested in investing in XRP.”

**Dash**
Dash was initially known as Darkcoin; it’s Bitcoin more secretive version. It offers more anonymity as it works on a network which is decentralized, hence making their transactions almost untraceable. Dash was launched in January 2014; it experienced an escalating fan following in a small span of time. Evan Duffield was the one who created this cryptocurrency, and it can be mined using a GPU or CPU. At around March 2015, Dash was rebranded from Darkcoin, which stands for Digital Cash and works under the ticker – DASH. Even after rebranding, they did not change any of their technological features like InstantX, Darksend, etc.
Ethereum

How to Mine Ethereum (ETH)
Mining Ethereum has become much easier than ever. You do not need to download the full blockchain, which is now over 25+GBS and still increasing. For the purpose of this guide, I will take you through the details on how you can self-mine the cryptocurrency right at the comfort of your computer.

The first thing is to download the following software to your desktop or computer.

- Download Ethereum software
- Setup Ethereum software
- Download mining software
- Setup mining software
- Mine

Step 1: Download Geth
Go to this link and download the Geth software to your personal computer. On the website, you will find the latest version that is currently available as Geth-Win64-latest.zip.
Geth is a program that is directly linked with Ethereum network. The software allows communication between your computer, its hardware, and the entire Ethereum network. Geth program enables your computer to pick up and pass on the mined information onto your GPU or CPU mining.

Step 2: Unzip GETH

The software downloaded will be in zip format because of its capacity. You need to unzip the GETH file and move it to a preferable location on your personal computer hard drive. (Right-click on the zipped file and select unpack).
Step 3: Start Command Prompt

The next step is to run the program you just downloaded. In order to perform the task, you will need to run the command prompt. You can easily do this by searching for the search function in a window for ‘CMD,’ then clicking on it when it appears.

Step 4: cd into Root Directory

When the command prompt is now open, it can look complicated for people who are not familiar with technical computer terms.

The command prompt box usually will have

```
C:\Users\Username>
```

In it is a box for the username, which should be the name you have assigned to your computer. Therefore, if you log into your computer with your username, crypto compare, then the command prompt box will open with

```
C:\Users\cryptocompare
```

Through a command, make your computer to find it in another place. The newly opened command prompt, types:
You should now see:

```
C: 
```

You will notice that you have used the `cd` command or change directory; a command that will turn the command prompt to look at the `c: /` drive.

Step 5: Create Geth Account

In this step, you will need to initiate a command on your Geth program to create a new account. It is important to remember the shortcut or the place you installed in step 2. This is as simple, as just case of typing in:

```
geth account new
```

Then press return or enter.

It should look like this:

```
C: \> geth account new
```

**Step 6: Create a password**

After pressing the enter button in step 5, you will be asked to enter a new password. In this platform, you need to know that, the system is set in such a way that you will not be able to see what you are typing in, so be careful. This password locks your account and keeps your private key safe.

*Remember if you accidentally lose this password, you will lose all your ethereum attached to that single wallet held by that private key.*

Once you have entered your new password and confirm it by re-entering the second time, you will have successfully created a new account. Bravo! You are about 70% done.

**Step 7: Connect to Ethereum**

Command your Geth program to start communication with the rest of the Ethereum network. For you to do this, you will have to type

```
geth --rpc
```
The results will look as below:

```
C:\> geth --rpc
```

Press enter, for the screen to start downloading the blockchain for Ethereum. At this point, you are synchronizing with the rest of the Ethereum network. For the process to be smooth, you will have to allow the system in your security firewall. Once you have just clicked, allow Access.

**Mining**

**Step 8: Download Mining Software**

At this step, you will now need to download Ethminer, which will make your GPU or CPU run the hashing algorithm, vital to securing the Ethereum network through the proof of work. The software can be downloaded [here](#). Remember to search on the bottom page to get the current best version before downloading.

![Ethminer Setup](#)

**Step 9: Install Mining Software**

Click on the downloaded file and install it to your computer. You need to remember that your firewall security can cause a challenge. Therefore, you need to allow the system to install and run freely. You should allow access if the firewall announces that a connection to the internet has been blocked from access. The same should be allowed if the window does not recognize or approve the software. Tell the windows it is OK if it asks. The process of installation is long, but you have to click through until Ethminer is fully installed.

**Step 10: Start command prompt**

You will need to open up another command prompt, as you did earlier in step 4. For an individual with little computer skills, you will see two scary looking boxes. Simply you will
have to click on your already opened command prompt, in the taskbar at the bottom of the screen page, and then click on the command prompt in the menu that appears.

A new command prompt should open showing the command below:

```
C:\Users\username
```

Remember this is the wrong place to find Etherminer. Therefore, you will need to tell it the right place to locate it.

**Step 11: Navigate to Etherminer directory**

When the new command prompt is opened type:

```
cd /
```

It should appear like this:

```
C:\Users\username>cd /
```

Then press ‘enter’ and something like this will appear:

```
C:\>
```

You will realize that you have just used the `cd` command, or you can change the directory command, to make the command prompt look as the `c:/` drive and not your user file.

**Step 12: cd into Program Files**
Type in:

```
cd prog
```

Then press the **tab**. This should look like this:

```
C:\> cd prog
```

Next press tab, which this will automatically complete the phrase for the closest fit, which will be found in the C: drive, just auto text the information on your phone.

After tapping a tab, you should see this:

```
C:\> cd "Program Files"
```

Tap ‘enter’, which should display a new line which looks like this one below:

```
C:\Program Files>
```

**Step 13: cd into Ethereum Folder**

Type in:

```
cd eth
```

Then press **tab**, followed by **enter**. This will take you into the newly installed Ethereum mining software folder.

Immediately after tapping tab, the software should look like this,

```
C:\Program Files>cd "Ethereum (+) 0.9.39
```

You should remember that the version numbers differ

When you press **enter** this should be displayed:

```
C:\Program Files\Ethereum (+) 0.9.39>
```

This will look slightly different depending on the version

**Step 14: cd Into Release Folder**

Type in:

```
cd release
```
Tap "Enter." This should give you the following:

```
C:\Program Files\Ethereum (++) 0.9.39\Release>
```

**Step 15: GPU mining**
Type in:

```
ethminer -G
```

Tap "Enter," and you should then start mining with your GPU, after building a DAG file, which can take around ten minutes.

**There can be problems at this point. For example:**

- Insufficient Memory
  The program might say that you have insufficient memory on your Graphics card to mine Ether, with Ethereum’s Ehash algorithm. If this is the case, you can still mine with your CPU, or go out and buy a new graphics card! If you get an error message like this, tap `Ctrl + c` to cancel the process. Then you can either retry it, or alternatively, move onto step 16, and mine with your CPU, rather than your GPU.

**Step 16 CPU mining**
Type in:

```
ethminer
```

Tap Enter, and you will start mining with your CPU. Create a DAG file, the first time you do this, which can take some time. After that is complete, your "Geth" program downloaded in step 1 should start talking to your "ethminer" program, and you should start mining!

**Litecoins**
It may seem difficult and expensive for new individuals without ASIC processors to start mining bitcoins. When this is the case, you need to know many other alternatives of digital currencies that you can still mine from your home personal computer. In this part of my guide, I will take you through what it takes to start digging up a few Litecoins without much costly extra equipment. If you have a spare AMD Radeon graphics card lying around, and energy rates that are not stratospheric, then mining a peer-to-peer Litecoin digital currency is within your reach.
Litecoin is a peer-to-peer network currency that allows instant payment to anyone across the globe. Its development and idea are based on bitcoin protocol. However, the main difference is that it can be efficiently mined with simple consumer grade hardware. In recent years, the rate of the transaction when using Litecoin has reduced to around 2 minutes on average. It uses the hard memory script based on mining proof-work algorithm which targets the regular computers and GPUs. From this part, you will realize that majority of computer users can be easily accessed with little effort. The Litecoin is scheduled to produce an average of 84 million currency units. Thus you need to grab a few bucks and store for your financial gains.

The main aim of developers who initiated the Litecoin crypto currency was to provide a mining algorithm that could run at the same time and within the same hardware as bitcoins. Bitcoin mining has now become a challenging task requiring heavy ASICS while Litecoin has in recent continued to satisfy these goals.

**Hardware you need to mine Litecoin**

You will need an ATI/AMD video card, which will cost you around $100 or more on it within the last few years. It has a higher end card to help mine Litecoin on windows faster. If you understand what video card you have, you can easily see what sort of K/Hs you require.

**The process of mining Litecoin**

**Step 1: download Litecoin wallet**

Before you begin mining, you will need a wallet to keep your hard-earned coins. You can download your wallet [here](#). This is a genuine link ensuring that you get the best wallet. Instead you can get the majority of the wallets on the original bitcoin-Qt client.
Step 2: install litecoin wallet

The process of installing the litecoin once downloaded is easy and simple. Next, click receive and later copy the address.

Step 3: Disable the antivirus

Many times the firewall security is not set to consider litcoin files. It is thus important for you to disable the antivirus slightly for the purpose of fully installing and running the litecoin software. The antivirus in many cases is picked up, and auto removed even before click on it or tries to open. This happens to all the bitcoin miner software. The reason this happens is because botnets tend to get the coins from zombie computer. You need to disable your antivirus for 20 minutes and add c:/litecoin to exclude it from scans.
If you have a different antivirus, it is good to Google and understand how to exclude a file or a folder from scanning the litecon files.

**Step 4: Download litecoin GUI Miner**

There are different versions of litecoin Gui miner ranging from 64bit and 32bit. You need to understand the specifications of your personal computer. This is important so as to install the right program that is compatible. You can download the Litecoin Gui Miner from this [link](#). It is a simple GPU miner.

Unless your computer has a specific mining hardware, the best miner to use is the central processing unit (CPU) or the graphic processing unit card. When you compare the two, GPU offers the best performance for the cryptographic calculations that is required. Remember that if you are a first time miner, your computer—a laptop should not have heavy games since this will slow the processors.

**Step 5: install and open litecoin GUI Miner**

Go to your folder and install the software, located in the `c:/litecoin`. Remember that if you would wish to change the location, make sure that you change the settings tab by pointing to mined in the new created folder.
The whole mining program should be downloaded at this stage. Some of other important mining programs that you need to have are.

- **CGMiner** - This is an important all round mining program, it was designed specifically for bitcoin, but can mine other scrypt up to version 3.7.2
- **Cudaminer** - This is a mining program for the Nvidia graphics card. You can now download it [here](#).
- **Cpuminer** - This is a mining program that is designed for use with CPU mining. It is much less efficient than when using a graphic card. To make your work easier I have the [link](#) for you to download.

**Step 6: Test litecoin miner**

right click, then paste replace the current address with your address you had previously copied in the step 2. Save and start process, and DOS screen will popup saying CGMiner

![GUI Litecoin Miner](#)

Immediately after cgminer.exe will start within 3 minutes, which displays on your screen like this verifies it. It will be showing you a GPU looking at the Kh/s Higher, which will ensure that more coins is earned in return. When you have verified it you will have to accept if it does not show this then you need to uninstall and reinstall your video card software with the ATI drivers as shown below and automatically this will work.
Step 7: set to run when system is IDLE

You need to right click, paste replace the current address with your address you had previously copied in step 2. **Save and start** the process, then Exit. This will run the process in the background.
Remember that different mining programs have different configuration processes.

**Step 8: start mining and get paid!**

Double click your.bat file to start mining. The command prompt window will display the result of your mining as it happens in real time. Depending on the pool you have selected, the miners will tell you the market value and all the entire information that you may need. This will take approximately 4-8 hours to see the results, which mean you will now be earning litecoins. You can monitor your payout status [here](#). Try to avoid running other programs in your computer when the mining process starts. This is because anything else that you run can only hurt your miners’ efficiency, and this attracts low profits.
You can also stop the mining process or all the running programs, by simply going to c:/litecoin/setupC.exe and clicking, End Process. Alternatively, you can open your task manager Ctrl+Shift+Esc and close CGMiner.exe and procesC.exe.

Mining litecoin as explained in this guide is so easy compared to other cryptocurrency, if you need more digital currency, more computer should be installed with the laid procedure. More computers set up more litecoins!

**Zcash**

Zcash is anonymous cryptocurrency that use zk-snarks to ensure that all the information regarding user transactions is safely encrypted, additionally; it is verifiable by a miner to ensure no double spending has taken place using zero knowledge proofs. Zcach uses equihash as a hashing algorithm; this is an asymmetric memory hard POW algorithm based on the generalized birthday problem. The algorithm relies on high RAM requirements, to bottleneck the generation of proof and ensuring that it’s making is unfeasible. This works similar to ethereum, which we discussed earlier in this guide.

Zcash mining is in recent times getting popular with solo mining and this is much lonely. You therefore need to test the waters on a zcash pool; this is good because you will be working in an environment where there are other miners.

**Reasons for mining zcash:**

- zcash is easily traded with other cryptocurrency like bitcoin, and this is a cheap way to slowly build up a holding position in bitcoin. For those who trade May understand that many bitcoin traders are bullish anticipating future price increase.
- BTC can easily be sold for cash, so if you mine ZEC, it will give you an advantage and an indirect way to fill your bank account at the time earning more cash. The currency can be sold for many major exchanges across the globe.
- Mining can be a great way to subsidize the purchase of a new, high-end GPU.
- Mining is considered the cheap way of entering into the zcash markets, which many traders love because of their volatility.
- When ZEC was first introduced in the market, it has been one of the highest priced altcoins in the current market.

Mining and holding the crypto is similar to the old adage where people used to buy low and sell high. However, most buyers do not know how to technically analyze, so we tend
to buy and sell at the wrong time. Buying gear and mining cryptocurrency with it allows you to own an income-producing assets in the gear itself. With holding resale value, very many times the value appreciates.

**Selecting your GPU Hardware**

GPU selections cards reveal the best card on basis of best price, performance and power consumption combination, mostly expressed as MH/s per currency unit. The best so far is the Nvidia cards popularly used during ethereum mining purposes on the ehtnashalgo. However, AMD cannot beat Nvidia when it comes to the equihash algorithm using the EWBF miner.

The card you decide to choose should have an average of 1GB of RAM; this is the best card for effectively mining the zcash. Remember that the EWMF supports GPU with just 1 GB of RAM, this is better when compared with 3 GB that ethereum required to run.

Use the following GPUs: Nvidia’s GTX 1060-6GB/1070/1080 Series; AMD’s RX 470/480, RX 570/580, R9 Series, or HD 7990/7950 (if used cards are available, try to get them from a gamer instead of a miner, with a warranty if possible).

For the best result and budget friendly, the Nvidia 1060 with 6 GB of RAM is the most recommended for mining process to take place without hitches.

**Mining Zcash on your PC**

In this part, I will show you in details how to mine zcahs with your CPU and GPU on the windows computer. The two miner software’s are important in ensuring you get the best from your effort.

**Step 1: Install your video card drivers**

AMD GPUs: you will need to download the software online from amd.com and install the GPU drivers. When you are at amid.com, choose support and drivers, enter your GPU information careful and then click display the results.
You can click on the download button for the current driver or select download previous driver and software on the far right hand side. This will allow you to select an older version that has greater driver for mining based on your computer card.

R9 and older: use 15.12

RX 400 Series: use 16.9.2 or 16.10.3

RX 500 Series: because these are newer, I would recommend going with current driver for now
Click on the orange button to start downloading

You will also need to download the latest Nvidia GeForce drivers. Go to this [link](#). Enter your card info, and click Start search. Your details and different versions will appear, you should download the current version from the result.
Install your GPU drivers as you always would do on other software and reboot your computer. You will understand that the GPU has been recognized correctly if you then go to device manager. Search it in the window search bar, and you see no warning from your firewall security.
Troubleshooting tips: Some miners have had problems after they have successfully installed all the GPUs, and the entire necessary driver. You should therefore find a way that suits you better by first installing one card. Then install drivers, shut down the entire system and later install the rest of the GPUs. This should be done if you have issues when installing the software’s. If one method fails to delete the files and start the other method. If you need to remove this driver, you will have to use the display driver uninstaller (DDU) program from here. This will remove the entire program safely and start a fresh.
Step 2: Get Zcah wallet address

This is necessary because you need a place to send the coins you mine. A zcash wallet is important for you to enjoy the profits. To find a safe wallet you will go to zcash, the official zcash website, and download the [zcash wallet](#). If you wish to use other wallets, you can also use hardware wallets such as trexor, ledger nano S or jaxx, these are few popular web wallets that you can use.

Step 3: Download the EWBF Zcash Miner

Once you have a wallet and address of your choice, the next step is to download the Miner. You should only download it from official threads in the bitcointalk. When you are in the page scroll down, you will see a couple of options. Use the mega download link to get the best version.

Always remember that the latest version is the best, download the zip file and then run it. Once you have it downloaded, extract it to your desktop so that you can easily manipulate and work on it. You will note that when you have download self-contained miner files, windows may provide a warning. If you have used EWBFs official download links, you can ignore this.

Step 4: Adjust your windows settings before mining

You will need to modify few settings from your computers window before you start the mining process. First, you do not want your computer to go into sleep mode, as it will interrupt your mining process. Go to your power settings and set turns off/sleep to never.

Then you will need to modify your entire system page file and manually set it to 16384 MB (16GB). Right click ‘this PC’ from windows explorer and choose properties. Click on advanced system settings. On the advanced tab, click settings on the performance section.

Click on the advanced tab and click “Change” under Virtual Memory. Uncheck “Automatically manage paging file”. Click the radio button for Custom Size and enter 16384 for the Initial size and Maximum size. Then click OK, Apply, OK.

You may also want to disable the windows updates. If you feel more secure, you can leave the updates on. However, remember the frequent updates will keep rebooting the system and stop your mining process.
If you run any antivirus on your windows, you should remember windows defender or some other antivirus program; add an exclusion to it so that it does not flag the entire EWBF folder.

**Step 5: Join a mining pool and configure your mining Bat File**

The next step is to set up a pool mining, this is important because you know solo mining is hardly going to make you a much cash as pool will, unless you have a warehouse full of GPUs.

You will need to choose a good zcash mining pool. There are plenty to choose from, but I can recommend Flypool. When you are at the site home page, you will find clear set instruction on how to mine on its pool using your EWBF Miner.

On the zcashes.flypool.org, you will find a section called window-Nvidia. The EWBF Miner is in this first section. You have to copy the miner script in the example below.

You will need to paste this string into the flypool bat file located inside the EWBF Miner folder we had extracted earlier. The bat file is a batch file that gives the commands to run the miner application.

Right click on the bat file named flypool and hit edit. The file automatically opens in the Notepad. Paste what you have copied from the flypool website. Update your server to us1 intends of what was then eu1 and remove the cuda devices language data at the end. The language you just removed is used to designate mining only to certain devices.
Next part is to copy your zcash wallet address. Inside the bat file paste your zcash address. Nice you have replaced your address you can also change the worker name to your personal preference. In this case its rig1, you can call it lets say ‘miningRig1.’

**Have your file as a batch file with .bat extension**

Choose File > Save As and type “.bat” after the name. In the Save As type box, make sure you select All Files, then click Save.

You now have a batch file ready to mine. Now create a shortcut for the new bat file and send it to your desktop. You can then delete the text version of the file.

**Step 6: Start mining**

Double-click your bat file to start the miner. The miner will start, initialize each of your GPUs, and hash away.

To monitor your earnings, go back to zcash.flypool.org and paste your wallet address into the Address window at the top. Then click Check Status:

**Welcome to our zcash mining pool**

That is all it takes you to mine Zcash.
Monero
Monero is a coin from cyptonite family. Its prominent feature is complete in traceability, ensured by the ring signatures, total security, and privacy. It is also based on the cyptonote algorithm. The reason as to why it relies on ring signature to provide a certain degree of privacy when making transaction. The currency is a good proof of work that cryptocurrency can be mined with computational power from a CPU or GPU. The crypto is good since it has no ASICS, which made it hard to mine bitocoin, only few with heavy machines can now enjoy the bitocoin mine.

When mining any crypto currency is to ensure that, you have to understand whether you will mine solo or via pool. As discussed in this guide, mining in a pool always attracts a fee but it is worth spend. When you decide to go solo, you will have to wait longer periods before you feel the reward of your efforts.

I would recommend you to use pool; this will reduce the variance and you in return have a steady flow of income. If you have good understanding of computational power, you can take advantage of solo pools, which functions well too. For the purpose of this guide, I will use monerohash, but you can use any pool you like. The fee is fair when you join monerohashl, the server is located in USA and you will only be charged 1.6% of the total amount. This is fair value when you compare the amount you will mine in the pool.

AMD Graphic card are the most optimal for Monero mining, it is also possible to mine with Nvidia GPU or CPU. In this guide, my aim is to ensure that you personally get the most profit, for that reason there are specific hardware, software’s created, and we will demonstrate on each options.

How to mine Monero
Part 1- CPU Mining

Step 1: download the mining software.

For this section of the guide you will use Wolf’s cryptonote. Open the source CPU miner; it is the one that provides the best results. Find the download link here.
Step 2: Extract the zip file.

Once you have downloaded the file, you will need to unzip it and find a folder like the one below.

Step 3: Now, when you are in the miner folder,

You will have to just extract the .zip file, you then have to hit ctrl+right MouseKey. You will be given an extra option that opens the command window. Just click on the command line and it will appear.
step 4: At this point our command line window (miner) is ready to go, all you need is now to type in the command line, “miner -a cryptonight-o stratum+tcp://monerohash.com:3333 -u YOUR_WALLET-ADDRESS -p x”. Remember that you have to replace your wallet address for your actual XMR wallet address.

The process is as simple as that and right away, you are now mining monero! You can view all of the commands that are available by typing “miner -help”. In our case we are just using the -a command, which stands for algorithm, the -o stands for server, the -u is your personal wallet address and the -p is your password, which can be left with an x when the mining pool does not need your login.
Part 2- AMD GPU Mining

Step 1: download the mining software

For this part of the mining we will need to use wolfs cyptonote an open source form AMD GPU Miner, this has in many times proven to provide the best results. For an approved and tested software use the link provided [here](http://www.example.com).

<table>
<thead>
<tr>
<th>Release 0.4</th>
</tr>
</thead>
<tbody>
<tr>
<td>Latest release</td>
</tr>
<tr>
<td><img src="image" alt="Release 0.4" /></td>
</tr>
<tr>
<td>OhGodAPet released this on Sep 13, 2016 - 6 commits to master since this release</td>
</tr>
<tr>
<td>Fixes lots of bugs with newer drivers - also adds a slight speedup, and many improvements like CPU mining from hyc.</td>
</tr>
</tbody>
</table>

**Downloads**

- wolf-xmr-miner-v0.4.zip 145 KB
- wolf-xmr-miner-v0.4.zip.sig 2.03 KB
- Source code (zip)
- Source code (tar.gz)

Step 2: Extract the zip file. You will be left with a folder similar to what you see below.
Step 3: configure the xmr.conf file

Now you will need to configure the xmr.conf file, open the file with the notepad, and change part of the url; "stratum+tcp://xmr.poolto.be:3000" to your pool address, in this case: "stratum+tcp://monerohash.com:3333". Replace the user with your wallet, in this case: "user": "45hVQbLnspDDViJeMc1v6mFPjKmJ38geKVZFRgFXxV1pVSDpG8jz4LfTmkvhgj9sPwjA1ZLJD9d3xTUF982Uk7poL2Ka94z"

Step 4: Go inside the miner folder that you extracted in step 3 from the .zip file and hit ctrl+right click mousekey. When you have done this an extra option will be given 'open command window here', click on it and a command line window will be displayed.
Step 5: Now our command line window is ready to work. All you now need to do is point the miner to the xmr.conf file; and then type “miner xmr.conf”. As simple as that you will now be mining with your AMD GPU. This in many times will give you the best results when mining XMR. However, when mining and you get a “clCreateBuffer” error, you need to lower raw intensity in the xmr.conf file “rawintensity” : 1336

Part 3: Nvidia GPU Mining

Step 1: download the mining software
For this section of the guide we will use the CCMiner version created and developed by tsiv, This is the one that provide best results when mining with Nvidia graphic cards. I have shared the link.

Step 2: extract the .zip file. You will be left with a folder similar to the one below.

Step 3: you now need to hit ctrl+right click mousekey from the extracted zip file and folder generated. When you have done this, you will be given an extra option “open command window here”. Click it, and a command line window will automatically open.
Step 4: Now that your command line window is ready, you now need to type several commands:

```
ccminer -o stratum+tcp://monerohash.com:3333 -u YOUR_WALLET_ADDRESS -p x
```

You have to replace "YOUR_WALLET_ADDRESS" for your actual XMR wallet address.

As you have realized the steps are easy to monitor and execute. You are now mining Monero with your Nvidia Graphic Card. Monero mining is easy with the variety of hardware. you can still give CPU a try, with the few steps.

**Part 4: Easy Mining with any hardware**

In this section we will use Minergate. You can also download it form this [link](#). This is a much easier way to use crypto currency miner, which will allow you to mine several crypto currencies with just a single click.

**Step 1: create an account with minergate.com**

When you visit the website, you will realize that minergate has its own in built wallet, in order to allow users to start mining even if they do not have personal addresses already set up. It is important to set a strong password because this is the only way you can secure your currency. You need also to activate a 2FA (2 factor authentication), which will prevent unauthorized users from accessing your funds even if they get to know your password.
Despite having an in built wallet, you need to understand that the safest place to store your funds is your own wallet.

**Step 2: Download the mingergate software and install it.** The website is developed in a way that it automatically detects the operating system and presents you with current version. Install and run minergate.

**Step 3: after you open and install the setup,** you will be presented with the option to start mining. Minergate automatically detects your equipment and selects the most profitable cryptocurrency to mine depending on your hardware make, difficulty, and price. Click smart mining
You can even choose how many cores you would want to use in your CPU and GPU. If your smart mining takes you to another crypto currency, you can pick monero manually.

![Smart Mining Interface](image)

It is as easy as that, you can now enjoy mining and making a profit.

**Ripple**

**Ripple XRP is not mineable**

Ripple is a global settlement network, that makes it easier to transfer almost all currency to anyone in the world in just a click of a button. The platform has rendered a conducive environment to send money; reducing the dominancy that was earlier enjoyed by SWIFT
or western union. Ripple has focused its effort in working with banks across the globe, offering them more efficient and cost effective way to send real time payment around the world.

Many banks are adopting the ripple system slower; this shows that the real time worldwide payments are the future. The ripple platform thus gives banks a unique advantage both over their competition and financially. The system focuses on the internet of value; this means that money transfer should move as quickly as how information moves in this technology age. With ripple, people will never again have to pay fortunes to send and receive money across the globe.

**Reason why banks are changing to ripple**
Several banks have now embraced the ripple platform. Among them include: Axis bank, Santander, Yes bank, Westpac, union credit, NBAD and UBS. The system is good in that banks can actually save an average of $4 per payment when they use the system protocol. If you can consider that banks perform millions of transactions every day, this will represent a significant saving.

The reason banks are adopting the system at an alarming rate, is how they can make more money, while saving more money. This is why Ripple is now considered a global changing system. It is the future that everyone want to be involved in. The new way of taking transaction is also bring the banking industry into the new modern internet age.

Ripple is continuing to hire the best top talent, who have improved the system across the world. The management has made it possible to make deals with banks, and this is a good thing in ensuring international payment is easy worldwide.

**How do I invest in ripple?**
Large scale investor has the capability of investing in ripple directly. Most of investors and speculators are limited to investing in XRP. Ripple’s native currency. Took off in value in the start of 2017 when it went from $0.01 to over $0.3 a coin. As it stands today, the ripple has the third highest market cap behind bitcoin and ethereum.
XRP allows for seamless financial transactions from any given currency to any other currency with negligible fees. XRP is the reserve currency that will allow users to trade nearly any currency of their choice into XRP and send XRP globally to anyone.

Every time any given currency is traded into XRP, liquidity increases, as does the total value of XRP, due to its greater demand. Ripple is now trying to turn XRP into a global reserve currency just like how the dollar has been in many years.

Transferring XRP is the easiest and least expensive way to send value over the ripple protocol. It is easy to move other currency using a platform that allows you to transact in a much easier way. This unique feature is what makes the XRP exclusively useful for global payments.

A long-term appreciation in the value of XRP is ultimately the end game strategy for Ripple, as they hold the majority of XRP in existence. This means that a bet on XRP is a bet on Ripple. It should be noted that Ripple also offers consulting services to financial institutions and has no problem securing funding when needed. In other words, it looks like Ripple is likely to be around for a long time.

**HOW Many XRP (Ripple coins) EXIST?**

100 billion XRP tokens exist; ripple holds 61 billion of them. The company holds the majority of the coins. This is to build confidence to the worlds investors. The system has locked up around 55 billion with 55 smart contracts. Each contract can hold a maximum of 1 billion XRP, and they usually expire up in the course of 54 months.

As it stands by now, ripple spent about 300 million XRP a month for the past 18 months to handle expenses. The openness in sharing the information is what is giving the investor a reason to believe that the currency is here to stay.

**Advantages of ripple**

Ripple is currently working with many banks across the globe which other currency have not attempted. Ripple is now focused on smart business where they ensure that no business can create bank cartel monopoly, the distribution of the currency will ensure that there is total corporation and easy control across the global finance.

The ripple is gradually increasing in value and dominance and this is a good reason for people to hold over a long time and reap the profits. All investors right now will be doing is to simply buying XRP, and forgetting about it and wait for the value to grow 10X or 100X.
Ripple transaction is steady fast and only takes a maximum of four seconds for a complete transaction. This is a good thing because you can use the currency to purchase the day-to-day items and can be adoptable by users worldwide. The currency is scalable, as it handles 1000 transactions a second. Compared to a visa, ripple can transact 50,000 a second.

**Ripples disadvantages**

XRP when it was created, all at once the ripple inventors owns the greatest majority of the tokens available. Therefore, this indicates that ripple has the majority control and may act like the central bank to manage the distribution of the currency.

University researchers have identified that ripple has several security vulnerabilities, when it comes to money, no one wants to think of its insecurity. This could actually prevent investors from buying and using the crypto.

Many people may decide not to invest in the XRP for reasons best known to them, others may fear to invest in ripple because in recent times people are using the crypto currency as an escape from banking cartels and constant government control.

**How to buy ripple in 3 simple steps**

**Step 1 - get ripple (XRP) Wallet**

The best thing to do when using this coin is to store your wallet in a hardcopy, let us say on a written paper and store it in the most secure place you can have. The XRP wallet works similar to the bitcoin and other crypto currency, therefore ensuring that you store it safe always. There is a requirement that every ripple wallet should be funded with a 20XRP reserve in order to protect it against low-level spam attacks.

Use ledger [Nano S](#) that is the only reliable hardware wallets for storing XRP and other crypto currencies.

Ripple offers a desktop wallet for windows, Mac, and Linux that give users a full functionality of the system. You can find the simple method guide to store the currency [here](#).

**Step 2 - Find a ripple exchange**

You can buy ripple with a fiat currency that is US dollar or euros, or you can trade bitcoind for ripple on any exchanges platforms.
Buy ripple with fiat currency
The best way to purchase ripple is to buy it directly through credit cards or through wire transfers using the Bitstamp. You can visit their personal website and get more details. When you sign up and follow, you will know your customer procedure. It will be easy to send EUR through SEPA transfer and USD by a bank transfer. Once you have transferred, fiat currency can be traded for XRP directly.

Gatehub is the other exchange that supports XRP. You will need to first sign up into their KYC process. Just like Bitstamp, Gatehub accepts SEPA transfers and bank transfers. The challenge with them is that they have a high bank fee transfer of $15. When you receive USD or EUR you can trade for XRP on their platform.

Buy Ripple with Bitcoin (trade BTC for XRP)
The management says that the easiest way to purchase XRP is by buying bitcoin from coinbase or another provider first. Then you need to send bitcoin to any exchanges and trade it with XRP.

The better way to trade Ripple with Bitcoin is through exchanging it on changelly or shapeshift. You can also buy XRP with bitcoins by trading it on poloniex and bittrex, among other big exchanges across the globe.

If you are located in Mexico, you can buy XRP from Bitso, while those residing in japan can use Coincheck or Bitbank to buy XRP. For the customers located in South Korea you can access XRP from coinone and Korebit.

Step 3- Withdraw Your XRP to your wallet
Once you have exchanged and received the XRP, it is good to actually withdraw it and save in a more secure private place. No matter where you received the coins always, remember to withdraw them and store into your ripple wallet that you personally hold the key.

In summary, you have realized that it is not possible for you to mine ripple but you can buy and own it. For investors, this is something to look at and invest early, the currency value will increase in due period and many banks will want to invest in it. For crypto currency fans, this is the time to take advantage of the low price, and invest wisely for the future returns.
Dash
Dash is a peer-to-peer open source, decentralized cryptocurrency that has a number of advantages over fiat currency and other cryptocurrencies. The dash core team, consist of about 100 employees who are continually improving the coin protocol. Dash was first introduced at a value of $11 in the beginning of 2017 and has increased its value to over $200 throughout the year making it one of the fastest growing crypto in the globe. It is the fifth altcoin.

Advantages of dash
According to the information shared on the dash website, it is a digital cash that can be spent anywhere. Dash has enabled a feature called privatesend that mixes coins through masternodes in order to make it nearly impossible to track a transaction from the beginning to the end.

Dash has also a special feature called instantsend, which allows payments to take effect within seconds and this prevents double spend problems, which is a common challenge to other cryptocurrencies. The transaction is secure across the world with the help of miners who collectively host the platform.

It is now easy to purchase items on a daily basis quickly with the use of dash coins.

Advantages of Dash over Bitcoin
Dash allows instantaneous, private transactions which is features not present with bitcoin, coupled with high quality security restored with the currency makes it better to the father of all digital currency bitcoin.

It is not possible to use bitcoin to buy day-to-day items while it is much possible to transact with dash. In terms of privacy dash beats bitcoin, the anonymity is highly enhanced in the dash.

How to mine Dash
Dash utilizes the XII algorithm during the mining process. Dash developers created this algorithm specifically to make it difficult for companies to manufacture hardware that solves it. XII consists of 11 different cryptographic algorithms, and this is mostly suited for
GPU mining rather than using CPU. GPU thus becomes much powerful when mining dash. As you can see, the use of GPU makes it easy for people to own the coin since it is decentralized, compared to bitcoin, which is mainly centralized.

**Requirements for mining Dash**

- dash core wallet
- windows computer
- Sgminer
- Time and electricity

**Mining process**

**Step 1: download dash wallet**

You need to visit the dash website and get your personal wallet; you can download the core program [here](#). When you download the core wallet, you will see something like the one below.
The program usually takes a lot of time, so patience is important here, once you open the program, it will start downloading the blockchain. Remember always to keep your wallet backup while using your dash, if you do not want to start losing what you earn.

**Step 2: Get SGMINER**

You need to visit Github link [here](#) and download the latest version of sgminer.
Be sure to extract everything and keep it in an easily accessible folder. Remember to use the link I have shared because there are so many viruses with sgminer, so be careful when you download. Sgminer is the main software that runs well with AMD GPUs when mining.

**Step 3: Configure Sgminer**

In the folder with dsgminer.exe, you need to create a text file named sgminer. Open the file and save as, select all files and save it as sgminer.conf. This is important because it acts as the configuration file when the program will be running. It will also communicate with the GPU and relay information on how fast the GPU runs. It also helps one to identify the pool and masternde to use for mining verification, and what is the best-mined Dash to be received and send.
First, you need to copy paste this in the text file:

```json
"pools": [
  {
    "url": "stratum+tcp://162.243.104.174:7903",
    "user": "XheyzUntHSgmglQo3NdNeOqLITiAAt1zhA",
    "pass": "",
    "algorithm": "darkcoin-mod"
  }
]
```

**Change the Dash Wallet Address**

Next, you need to open your Dash core wallet and get your receive address, follow the information above for much details. Clicks receive and then copy the new address and paste it in between the quotations on the sgminer.config file.

**Select and setup pool**

You need to select a pool. This is important because it helps you get your share of mine dash; also a pool makes the payments faster than when you are mining in a separate way. When you use a pool, you will have to spend a few bucks and the process in many times is centralized. You can use the list masternodes to find the closest node to you. The best node is the one with the lowest latency, once you find one, copy the IP address, and paste it where pooladdress is in the config file. Remember to paste it without editing the rest part.
**Step 4: Run Sgminer and start mining**

In this step, you will notice that you have configured the dash miner on your computer and connected it to the dah wallet. Go to your installation folder and run sgminer.exe. If all is well, the system should look as it is below.

In case of a crossfire setup, please do remember to disable crossfire in your ATI catalyst setting. AMD catalyst drivers 14.7 RC3 is 15% quicker than version 14.7 RC1 using Wolf0’s bins, but 14.9 may cause instability issues especially with older cards running together with R9's.

**How much you will be earning mining dash**

When you run, the sgminer will give your hashrate an upper hand. The profits will be estimated from the Mh/. Using the dash calculator, the estimated profits table will look like this at 6MH/S
Sometimes mining can be a challenge to many, others especially those with little computer skills would prefer to buy.

**Steps on how to buy dash**

**Step 1: Get a dash wallet**

Just like any other digital currency, you will need first to get a wallet. There are so many different types of dash wallets out there. If you prefer to have large amounts of dash, it is good to always go for a hardware wallet, otherwise just go for the mobile or desktop wallet.

**Dash desktop wallets**

The best desktop wallet for the dash is the electrum dash wallet, many windows version can support the wallet, but you need to know that the wallet does not support special features such as Instantsend and privatesend. The best wallet so far is dash core wallet, which is available for Mac, linux and for windows.

**Dash Hardware wallets.**

You can use the following dash hardware wallets, [trezor], [keepkey] or [ledger], they are the most secure and can use and store dash for a long period of time.

**Dash mobile wallets**

With the technology age, there are several good android and iOS dash wallet available. [Jaxx] is one of the best that I can recommend for iPhone and android users. You can also
check coinomi, which is considered best for making good wallets for both android and iPhone.

**Step 2: buy Dash**

It is easy to exchange bitcoin for dash in different exchange platforms such as changelly and shapeshift. All you need is simply trade bitcoin for dash and right away you have it, transfer to your private wallet for storage.

**Purchase dash with a wire transfer**

Bitpanda and kraken allows you to buy dash using your credit card, skrill account, SEPA transfer or SOFORT transfer. Buying on Bitpanda it will only require a personal verification and has a buying limit of 600 euros. Kraken on the other hand allows you to fund your account with both USD and EUR.

Buy dash directly with cash

There are three locations in the United States, in Oregon, Florida, and New York, where users can buy Dash directly from an ATM. While the fees are high, this is one of the easiest ways to acquire Dash. ATM locations to purchase BTC and other cryptocurrencies can be found at CoinATMRadar.

For those using wallofcoins, you only need to deposit cash at a local bank and buy dash directly to your personal wallet address.

**Step 3: Move the dash coins to your wallet**

This is the most important step that you should always remember once you finish buying dash, move it to your personal wallet. Leaving coins on an exchange is easy get lost or stolen.

**Dogecoins**

Dogecoin is a decentralized, peer-to-peer digital currency that allows people across the globe to send money online. Compared to other cryptocurrencies, dogecoin has had a fast initial coin production schedule, whereby over 100 billion had been circulated by the mid 2015 with an additional of over 5 billion coins every year.

Dogecoin mining is possible with highly specialized computers and hardware’s, which serves two main purpose. I.e., ensuring that the network is carried in a secure place and the combination is used to pay out rewards to miners.
How to mine Dogecoin guide
If you have carried research, you will realize that dogecoin has only been in existence since December 2013, and it is already the third most popular cryptocurrency after bitcoin and litecoin.

What you need to start mining
You will need cheap electricity and a few graphic cards to start you mining. However, you can still start mining dogecoins using your single personal computer. It is also possible to mine without graphic cards, although the entire process will be slower.

Compare your setup with the litecoin mining hardware comparison page found in the link shared here. The reason you comparing with the litecoin is because dogecoin design is based on it, the values will help you understand the relative power of your hardware you will use to mine.

First, you will find your graphics card or CPU model in the column, and then you need to check the next column for KH/s value. This is a measure of the speed in which you will complete hashes. For better results, you will need something that has at least 150-250Kh/s to be able to mine a few number of coins. You need to remember that the faster the cards the more electricity is consumed.

Step 1: download dogecoin wallet
First, you need to visit the official dogecoin page and download it. Later install your personal wallet. For the purpose of this guide, I will be using the dogecoin core wallet; you need not to worry since all the wallets share the same basic features. When you install your wallet, click on much receive to view your wallet address.

At this point, you should encrypt your wallet from the menu setting. This is important in securing your computer and coins in case of a computer hack or infection by wallet seeking malware.
You can realize that once you install the doge wallet, it has to synchronize with the network. That is the reason why the wallet will be catching up with all of the historical dogecoin transactions in order to see if there is any related to you.

**Mining pools and solo mining**

Mining doge involves your computer finishing a block of mathematically designed puzzle and later receiving a reward for solving it. The challenge is that it is difficulty to solve a single block and thus solo mining is a challenge to complete, thus it will take longer period to mine.

On that note, it is advisable for you to join a pool and reduce the duration it will take to get rewarded. To join a mining pool you just sign up on their website, and remember to select the best pool that charges an affordable amount and has clear instruction and support.

if you are a beginner you should join pools that mine coins on the X11 algorithm which automatically payout in doge. These are the few mining pools you can join as a beginner, [https://www.multipool.us](https://www.multipool.us) and [doge.hashfaster.com](http://doge.hashfaster.com). Both the pools are easy to use, and the registration process is easy too.

**Step 2: set up a mining program**

Select the server. For the X11 ports, use the one with the lowest difficulty, select Doge as payout currency, and add a wallet address that you have setup in your wallet.

**Step 3: download a miner program**

At this step, you will need to download miners that support X11 algorithm, to easily get one visit the doge official website. After downloading the miner, you also need to install it by following right config details. The extract syntax is different depending on the miner. When you use cpuminer it will look like this.

```
miner -a X11 -o stratum+tcp://ca.simplemulti.com:3453 -u walletaddress -p worker1 -t 2
```

**Step 4: join a pool**
To join a pool, select one from the following lists and sign up for an account. You need to remember that larger pools are good to join since they offer more payouts that are consistent.

Doktorrf pool directory

Doge pool directory

It is not advisable to sign up in more than one pool since this will confuse you when you start mining. When attackers want to hack, they will look for username with same name and password.

Making workers

When you join a pool, you need to log to their webpage and create a worker for each graphic card or CPU you have for mining. Select my workers, on the left hand side, you can find it under my account.

On your worker dashboard, there will be an option to create a new worker account as shown below.
You then give the worker a username and a new password. Once you have added your new worker, you should see it added to your list. Repeat for as many graphic cards / CPUs you plan to have mining and note the usernames and passwords. You can always come back to this page if you forget.

Now go to getting started which is located on my home or sometimes help. All the pool you have joined will have at least one stratum with a corresponding port number.
Step 5: set up a cgminer (AMD hardware on windows)

First, ensure that you have the latest drivers for your graphics card by downloading the latest version [here](#). For those with little computer skills you can go to your device manager, click on the control panel and select the hardware and sound, then click on device manager. You will be able to find the best version that suites your computer.

Once you have installed your latest drivers, you need to also download AMD SDK from the link [here](#).

Once the SDK is installed, extract your downloaded cgminer file (link in the software section) to a location you can remember. Next, open up notepad and paste the following,
replacing your-pools-stratum, port-number, web-login, worker-name, and worker-password with your information:

```
setx GPU_MAX_ALLOC_PERCENT 100

```

It is basically saying use 100% of your gpu, scrypt mode (gpu mining), intensity of 10, target temperature of 70, GPU fan speed at 10-70%, then the stratum connection and worker information. Be sure to watch the temperature even with the fan settings, some cards do not respond to these commands.

Now go to save as, from your cgminer folder, select the all files dropdown, and then save it as anynameyouwish.bat. This will create a window batch file, which runs cgminer.exe with the provided commands prompt.

Run the batch file you have created above and this should now work well with the cgminer. When you run the batch file, you should able to see something similar to the one below.
Step 6: Get paid

Once you have run the system, you should now check if you have mined some coins. Login to your pools web interface and go to edit account; it is located under my account. Give it an address to send your coins, then you should configure an automatic payouts, this can be set manually.
Chapter 8: The Network of Bitcoin

Bitcoin works through peer to peer transaction. This network is created while transferring Bitcoins from one person to another. Every transaction, however, depends on the specific features of the model being used by the two peers. For every Bitcoin networking model to be effective, each peer must provide a destination of the participant. The Internet is the key factor running the entire transaction. Why is the transaction referred to as peer to peer transaction? Well, the reason here is that there is uniformity for the networking computers participating in the transaction. This means that the two devices are similar in all aspects, with equal nodes that play a role in network services provider.

The special thing with these nodes sharing the network is that they function on a flat topology; a mesh network controlling all the activities of the transaction. Therefore, performance is on equal chances with no participant on top of the other. The services are never centralized, and there is no server for central monitoring of the transaction. Networking, therefore, ensures transparency of the transaction and a mandate for each participant to exercise full control over the entire transaction. The sharing nodes make this possible. During a peer to peer transaction, the
networking nodes for both the participants will produce and consume services simultaneously. Participation Incentives are earned as reciprocal of the undertaking.

**Features of the peer to peer network**

The major feature of the peer to peer transaction networks is that they are decentralized. This is the control factor of the Bitcoin industries, making the entire process remain on flat topology level. No hierarchy of participation, in that no one is on the top of the other, but instead, everything is taking place at the same level. Additionally, peer to peer transactions networks are open and inherently resilient. Some years back the peer to peer networking worked on a pre-eminent network of the early internet architecture, with equal computer networking nodes. Today, though the topology of the internet protocol is on the same level, the architecture of the internet has been modified to be a bit hierarchical.

**Bitcoin peer to peer network and protocols**

Bitcoin network can be defined as a group of network sharing nodes that run the peer to peer transaction of the Bitcoin. Bitcoin network involves other protocols being bridged by the gateway routers to the major Bitcoin protocol. Example of the intermediate protocol is the stratum protocol. These are networking protocols for the mobile, and lightweight wallets, as well as the protocols, used when mining. How does the stratum protocol get to the major Bitcoin protocol? Just as mentioned earlier, stratum protocol is an intermediary connecting other activities to the major peer to peer Bitcoin network. Through the peer to peer Bitcoin protocol, the router servers are able to reach the Bitcoin network. This provides a network extension to the sharing nodes in order to run the network to the other protocols. For instance, the mining nodes of a stratum are connected via a routing server to its protocol, which then connects the protocol to the major Bitcoin network and finally it is bridged to the peer to peer Bitcoin transaction protocol. A Bitcoin system is, therefore, an extended network connecting the overall transaction network; the P2P Bitcoin transacting protocols and the subset blockchain protocols such as the stratum and the pool mining protocols.

Besides being decentralized, Bitcoin networking is beyond being a flat topology. Well, you could need a simple reminder of Bitcoin to understand well what flat topology network is all about. To be simple and precise Bitcoin is a digital peer to peer designed cryptocurrency system. More so the network architecture for the transaction is founded on the reflection of the latter. Enhancing a decentralized system is the main focus in Bitcoin networking. It is designed to enhance a flat topology and to avoid centralized networking consensus.

**Networking nodes and their functions**

Bitcoin cryptocurrency networking nodes refers to a package of functions of a Bitcoin network. These include; mining, routing, providing wallet services as well as provision of a blockchain database. Not forgetting that the Bitcoin peer to peer network is decentralized and that they function on a flat topology, the network nodes, however, tend to assume different functions based on their supportive roles. Therefore every network covers a full node of functionality. This full node
is made of four features which are; a wallet, network routing node, a miner and the full blockchain database.

Apart from route network functions, the nodes may include other different functions. Generally, the network nodes will assist in propagating and validation of both the blocks and the transactions. The nodes will also function by discovering peer to peer connections and maintaining the connections. Peer to peer connections is dependent on the blockchain, and it should always be updated. A full node will, therefore, ensure that the blockchain is complete and updated regularly. Moreover, the full nodes will help in maintaining a decentralized functionality of the cryptocurrency Bitcoin network by conducting an independent autonomous and authoritative verification.

**Simplified payment verification nodes (SPV) and Lightweight nodes**
The simplified payment verification nodes and the light nodes are minor protocol nodes. These simple nodes play a great role in controlling the functioning of a single subset of the entire blockchain. SPV will thereafter verify the payment of such transaction. Normally, to differentiate the full node and simple nodes, the full blockchain for the full node functioning database is circled with different colors and indicated full blockchain. The lightweight nodes and the simplified verification nodes have different colors drawings to distinguish from the latter and an indication that they only have a subset copy of the full blockchain.

**The mining nodes**
The function of the mining nodes is to create brand new Bitcoin blocks. The networking nodes work with the aid of hardware which when run will compute the maths and build Bitcoin blocks through the display of a proof of work algorithm. Mining nodes are made of lightweight nodes; for a subset copy of the blockchain and a full node with a complete up to date copy of the entire blockchain. Lightweight nodes function mostly in pool mining and use router server to connect them to the main Bitcoin full node.

**Wallet**
Many refer to it as the user wallet since it contains the user’s destination address. Example of the user wallet is the mobile smartphones among other devices such as the laptops and the desktops. A user wallet may display full node or lightweight node functionality. Most interesting to note is that similar to the many clients participating through desktops; user wallets will mainly display a full node networking. Most of the user wallets with lightweight and simplified payments verification nodes are those that use such devices as mobile and smartphones. This is because they strain their resources a lot as compared to other devices.

The protocols subsidiary to the main Bitcoin peer to peer transaction protocols are run by the servers and lightweight nodes. Such networking nodes are the lightweight protocols for client
access and the mining pools special protocols. Therefore, note that the Bitcoin network for extended networking contains the following types of nodes and their functions.

**Bitcoin core**
This is the reference client network which contains the user wallet, node for network routing server, full blockchain database and the miner necessary for peer to peer Bitcoin network.

**Full blockchain node**
The full blockchain node for Bitcoin peer to peer network is made of the network router node and a database full blockchain.

**Solo miner**
The solo miner is made of the full up to date blockchain copy, mining functions and Bitcoin peer to peer network routing node.

**Lightweight wallet (SPV)**
This may not contain the full node blockchain database but has the network routing node on the peer to peer Bitcoin network and a user wallet.

**Pool protocol servers**
These are the gateway routers connecting the major Bitcoin protocol to the other protocols. i.e. they offer connectivity of Bitcoin peer to peer network to the rest of the nodes running other protocols. These include the stratum and the pool mining nodes.

**Understanding Extended Bitcoin Network**
An extended network consists of the network running the main peer to peer Bitcoin protocol and different nodes used in running various protocols. The lightweight nodes also known as the simplified verification nodes are joined to the peer to peer main Bitcoin network. These are the pool route servers and the gateways for the subsidiary protocols. Others include pool mining protocol nodes, the lightweight user wallet client protocols among other protocols without a full copy of database blockchain.

According to the full node Bitcoin network, a maximum of 10000 nodes and a minimum of 7000 nodes are necessary in order to run peer to peer Bitcoin protocol among other versions of the Bitcoin core or references. The BitcoinJ, btcd and the Libbitcoin add up to few less than hundred nodes implementing various auxiliary peer to peer transaction Bitcoin protocols. Other mining nodes represent an insignificant percentage of the main peer to peer transaction Bitcoin network. Both offer stiff competition invalidating of the mining process and transactions, ensuring verifications and creating of brand new Bitcoin blocks.

Most of the large companies operating Bitcoin peer to peer transaction network run full node Bitcoin references. These contain a full up to date blockchain copies and a main Bitcoin network node. However, this does not contain the user wallet functions or the mining details. Except other
nodes, the nodes for the interface of the large companies are also referred as the edge router network. These give room for the other services such as the processing of the merchant payments, making exchanges, block exploring and verification of the user wallets.

**Network transactions**

Bitcoin transactions revolve along networking from the individuals. Every transaction is different depending on the networking model. Various transactions outline the peer addresses indicating the transaction source as well as its destinations. For a single transaction, there is two destinations and more than one addresses. Your peer partner to where you are transferring your Bitcoins becomes your first destination.

The second destination represents the user wallet addresses, while the third destination is not determined by either of the two peers. It represents the address of the intermediary arising in the transaction especially when the destinations of the two transacting peers did not add up. This could be the scenario introducing the third destinations. Ann and Isaac are carried out a Bitcoin transaction where Ann sent 100 Bitcoins to Isaac. For this case, Isaac address is our first destination while Ann’s user wallet address where the 100 Bitcoins are being charged represents the second destination.

A situation may arise where martins address shares the same wallet with ann.in such a circumstance, the three destination will contain the following Bitcoins in their addresses; Ann address 150 Bitcoins, Isaac address 100 Bitcoins and martins address 49.5 Bitcoins. The missing 0.5 Bitcoins represents transaction fee payment to the miners. Once the mining activity is over, it is encrypted for network submission and continuity of the next step which is confirmation. This occurs when the network takes the encrypted transaction and it is added to the already existing block. It is only after the transaction has been fully encrypted in the current block chain when Isaac is able to claim the 100 Bitcoins sent by Ann as his own.
Bitcoin-QT is the software installed in the device of the peers. With it, the user wallet is safe and secure on their devices. The software moreover creates a peer to peer network node that helps in blockchain distribution. This node signals a working command hence mining starts once the node is used to register a miner. The two peers can now request to start mining. The lottery won during mining help in boosting the processing power of the network. After every mining activity, the miners get hash as a form of payment.

**Exploring Bitcoin networking blocks.**

As discussed earlier, it is clear that after every mining activity a hash is produced. In case the hash produced as a lower value compared to the block found previously, then, a new Bitcoin block has been discovered which should then be passed for submission and verification. The P2P network has also to confirm the newfound block to allow for the closing of the old block and opening of the newly discovered block. After that the founder of the block is awarded. Well, a transaction shall be considered confirmed in case the P2P network has attained a total of six transactions confirms achieved by the creation of new blocks. Confirmation plays a vital role in ensuring that double spending does not occur during a transaction.

The maximum numbers of the bit-coins in the Bitcoin industry are 21,000,000 BTC. After every transaction, the reward has halved a technique used to ensure that the Bitcoin value keeps on increasing. Therefore, even with the most insignificant Bitcoin reward, it is sufficient enough compared to the government currency hence participants will always be attracted to the market. Currently, one Bitcoin is worth $200, hence with 10BTC is equivalent to $2000. Each day, a system releases a fixed amount of Bitcoins.

**Bitcoin difficulty networking factor**

The ease at which the P2P network finds a new block is controlled by a factor referred to us as difficulty. The level of difficulty is changed after every 14 days or every time 2,016 blocks are created. To determine the processing power of a system is done by calculating hash rate or hashes produced in every second. Hash can, therefore, be defined as taking computer algorithms inputs, carrying out math computations on the same and coming up with a long string representing it. Bitcoin uses SHA 256 hash, a notation of Hex-Decimal representation with 64 characters ranging between A-F or could be 0-9.

Use of hashes in the Bitcoin industry is important as its verification is less complicated and it’s impossible to reverse the payments when using it. Currently, hash rate is measured using TH/s. You will, therefore, encounter such mining units as Hashes per second; H/s, Kilo Hashes per second (KH/s), Mega Hashes per second (MH/s) and Giga Hashes per second (GH/s) and Tera Hashes per second (TH/s) and Peta Hashes per second (PH/s). These measures of units relate as follows.

\[
1,000 \text{ H/s} = 1 \text{ KH/s} \\
1,000 \text{ KH/s} = 1 \text{ MH/s}
\]
Networking through pool mining or solo mining

A miner can either carry out solo or pool mining. Whereby solo mining means individual based mining in which the miner will connect his/her device to their networking node, and in case they create a block, they receive a reward. On the other hand, pool mining involves a group of miners mining together, who share the reward by splitting it equally in case they find a block. Whether a miner in a group of pool found or did not find the block, they still stand a chance of being paid in relation to the contribution they offered. Example, Ann, and Isaac have the same hash Power of 2.1 GH, and they get indulged in pool mining each earning 40 BTC for the contributed efforts.

Isaac did not find any block while Ann was able to find three. One of the blocks Ann found was 50 BTC and the other two blocks were 25 BTC each. In such a situation Ann will only receive 40 BTC while the rest 100 BTC are taken to the pool. Unlike for the case of pool mining Ann would be rewarded for the blocks, she found it was Solo mining. Moreover, if Ann found the block in the pool, the poo operator receives the reward for such a discovered block. Ann will also benefit from finding the block as each transaction for each founded block is included in her block if she was solo mining. However, the pool operator will instead earn the fee in case she was involved in pool mining.
Chapter 9: How to Predict Return on Investment and Payback Period of Cryptocurrencies

Investing in cryptocurrencies
At the beginning of April 2016, the total cryptocurrency capital market was estimated to be around $ eight billion; currently, it is just over $ twelve billion. This shows an over 50% increment, nevertheless, this can be misleading. An understanding of the crypto-coin content and expertise in the investment field is required to obtain optimal exposure into blockchain technology investment. The technologies pushing these cryptocurrency works requires more than just transactions. In future, we will witness all-around better solutions. For a prudent investor, the vital thing is to determine the cryptocurrency that will cater for the true need and not just a fad of a short period.

In the investing world, we have several general rules to follow. However, some are more important than the others are. One of the key things to consider is the longevity, not just of the product, but also the producer of the product. For how long will the service be relevant? How is the ease of the competitors to out-perform this cryptocurrency? Are the developers committed?

Therefore, the key issues we are looking here are
1. A growing and current demand for it.
2. No evidence of imminent competing threats.
3. A team of developers who are committed.

With all this on the cause, then there is a potentially good risk to rewards.

Another big thing to consider is always seeking platform and not features. Most cryptocurrencies are feature works. That explains why only around 30 of cryptocurrencies are viable today. The other 720 plus are useless long-term investments. Coins like Bitcoins and Ethereum have enormous momentum, backing, and multi-cryptocurrency wallet and are examples of platform-based work; they are easy to be operated by the masses and avails a real-life use case.

**A statistical analysis of cryptocurrency**

Understanding the risks involved in any investment is very vital. This is done by analyzing statistical properties of this cryptocurrencies as determined by market capitalization. Their exchange rate is versus the US dollar. Returns are non-normal; nevertheless, no one distribution fits well jointly to all blockchain technology analyzed. For the commonly used currency like Litecoin and Bitcoin, the generalized hyperbolic distribution gives the best line of fit. For the smaller blockchain technology the generalized $t$ distribution, Gaussian distribution, and Laplace distribution give the best fits. The results are important for risk management purpose and investment.

Bitcoin, as the first decentralized blockchain technology, has benefited greatly from the financial industry, academics, and the media. It has set itself as the leader of the cryptocurrency and is not going to slow any near soon. Growing need for Bitcoin has skyrocketed in the recent months like for example the UK federal government is considering paying out research grants in Bitcoins. So many IT companies are stockpiling on Bitcoin to shield against ransomware. Chairperson of the board of governors of the US Federal Reserve has encouraged central bankers to study the new innovations in the industry.

Many cryptocurrencies have emerged. However Bitcoin remains the most popular with cryptocurrency market representation of 81%. The main six cryptocurrencies, which have stayed for over two years and covered 90% of the market, include Bitcoin, Litecoin, Ripple, Monero, Dogecoin, and Dash. The data used in this statistical analysis are the historical global indices of cryptocurrency for a period of over two years. Most cryptocurrency exhibit heavy tails. The results obtained after the analysis indicate that none of the distributions that were used gives the best fit jointly for all cryptocurrency.

Litecoin and Bitcoin had the best line of fit using generalized hyperbolic distribution. Ripple, Dash, and Monero had the best fit using the normal inverse Gaussian distribution. Dogecoin had the best line of fit using $t$ distribution. The outcome of this results are in areas of risk management and also for the purpose of investment.
Ideal investment strategies
Ethereum and Bitcoin are highly disruptive cryptocurrencies by looking at the advantages of blockchain technologies that drive technology in numerous industries. To come out with an ideal investment strategy, we analyze the historical performance and the extrapolated performance of this cryptocurrencies. Working with the industry professionals has helped to identify the most impactful and probable factors for the future demand of cryptocurrency. Cryptocurrencies speculative nature and volatility create a need for diversification across platforms.

Fiat currency comes into existence because it was able to be controlled and regulated by governments. Nevertheless, it comes with a set of issues. As a way to fix these issues, there was emergent of cryptocurrency around the year 2009. This is a leveraged disruptive technology called blockchain.

In the recent times, the popularity of cryptocurrency has increased. This has prompt investors to determine how to invest into this asset. As a new technology to invest in it, there are many factors to consider to predict their future. To make an informed decision, it is important to check the potential applications, network difficulties and other foreseeable limitations in future as well as origin of the technology. We aim to predict the price of Bitcoin and Ethereum in the next five years through a qualitative and quantitative analysis. From this prediction, we will be able to make appropriate investments.

Bitcoin is the most used and widely known cryptocurrency in the world. It has a current capitalization market of over $10 billion (cryptocurrency market capitalization 2016). The original
aim of creating Bitcoin currency was to eliminate trusted third party financial institutions. Bitcoin achieves this by, increasing efficiency, eliminating the possibility of fraud and providing security and validity of a transaction. Bitcoins work by increasing efficiency and reducing unnecessary costs and time of using several financial institutions to equip transactions. Bitcoin is very adaptable in the markets which lack customary financial infrastructure but do have access to mobile data and markets with high and inflated currency which require equipment to allow for the exchange of currency and mobilization.

Ethereum, on the other hand, has the advantage of the application of Smart Contracts within its code. The total market capitalization of Ethereum is approximately 10% that of Bitcoin. The appreciation and depreciation value of Ethereum lies in its ability to eliminate financial institutions in future.

Bitcoin and Ethereum are both mined by solving complex computational problems. Both have additional difficulties in mining as more blocks are added into the blockchain.

Using historical data to predict values for cryptocurrencies is very difficult since there are no sufficient data to extrapolate future prices without a doubt. By examining the trend of the price of Bitcoin in five years is $2250 representing a growth of 301 percent. Ethereum has an extrapolated five-year value of approximately $ 88 that represents growth of 634%. This shows a tremendous growth rate, which is as a result of adoption and hype in the early stage of its life cycle. On deeper analysis, this volatility and high growth of Ethereum and Bitcoin is as a result speculation and hype. This is indicated by the high correlation between Google search and prices of Bitcoins. The time series correlation between Google search and price is 0.64 for Bitcoin and a higher value for Ethereum of 0.88.

For the purpose of accounting for the hype in the regression forecast, the importance of spikes as a result of increased hype and Google searches were discounted by a value of 30 percent. The prices are very much depressed when speculation and hype covering each currency is decreased by a factor of 30 percent. There was a growth rate of approximately 300% for Bitcoin and reduction of 506% for Ethereum on depression impact of Google searches. Even though the reduced importance speculation and hype does lessen this prediction of Ethereum, it has experienced more growth, especially in the recent past.

Speculation-Discounted Price model (bitcoin on left axis, Ethereum on right axis, in USD)
Even though Ethereum looks like a better investment in regard to this analysis, past result do not indicate future performance. Again looking at the high volatility of these currencies, and absence of extensive history this predictions cannot be relied on in the final decision.

In order to have a strong prediction, talks and interviews were arranged with several professionals and experts of cryptocurrency as well as enthusiast traders. Every individual was polled on probability of various occurrences, which affect the demand of every cryptocurrency. They were also required to rate the probable level of impact on the cryptocurrency.

**New markets**

Countries with less developed financial infrastructure but with high smartphone usage are potential markets in which cryptocurrencies can be leveraged. A good example is Kenya where half of its GDP is operated by digital currency. Such countries can take advantage of cryptocurrency in terms of moving money in and out of the country. Bitcoin can offer a great potential for the upcoming markets, as it is widely adopted cryptocurrency. There are over 14 million Bitcoins in circulation with the lowest level of volatility and the highest level of adoption.
Financial institutions
There has been willingness by the financial institutions to adopt cryptocurrency technology. This is a move to access untapped markets and drive operational efficiencies. But large financial institutions have shown unwillingness to adopt a specific currency. Even though cryptocurrency technology is very likely to be adopted by financial institutions, it is very unlikely that Ethereum or Bitcoin currencies will be widely taken by these organizations.

Regulations and deregulations
Permissive regulations in the western countries has benefited Bitcoin. Nevertheless, it has experienced restrictions in the western countries. The banning of Bitcoins in China greatly affected its value price. This indicates the importance of global acceptance of cryptocurrency to push up its value.

In order for cryptocurrencies to receive a wide world acceptance, there must be regulations to ensure secure and safe transactions. Deregulation would cause a significant value growth of Bitcoins and ease of transactions across borders. On the other hand Ethereum will not have much value addition, but will experience widespread global adoption.

Major network compromise
In such a highly complex network with the anonymous exchange of data, the chances of ‘hacks’ as an example of network compromise are very high. Ethereum has experienced hacks where a significant amount of ether units has been siphoned. Such a major hack is quite unlikely to happen with Bitcoin because of its rigid framework and relative Lack of widespread utility. More freedom, more nodes and the higher the chances of hacking as in the Ethereum network. Risk of hacks is evident in both Bitcoin and Ethereum trades. However, this is not an indication of flaws in blockchain technology. History has shown that hacks do affect the price of each cryptocurrency.

Global economic event
The utility of Bitcoin is strictly digital currency. Due to this, it is expected to have an inverse relationship to the state of world economy. Areas with highly inflated currency or lacking financial infrastructure can use Bitcoin as an alternative means of transaction. Ethereum also has an inverse relation, but with lesser magnitude due to innovative nature of Ethereum network and a wide array of uses. Bitcoin values act like commodities while that of Ethereum relate closely to widespread adoption of the network as well as smart contracts.

E-commerce
Both Ethereum and Bitcoin exhibits potential of their values to be positively impacted by e-commerce. Nevertheless, Bitcoin stands a higher chance to be used for trade. Payment systems are in such a way that they take a long time to be processed. Cryptocurrency reduces this transaction time. Bitcoin offers a better solution for this unlike Ethereum, which has a greater potential for hacks.
Financial technology
The cryptocurrency applications for financial applications favors more the Ethereum as it is more flexible for the institutions to carry out operations. There is a secure transaction as well as a single ledger that shrinks the need to reconcile across every party independent ledger. Individual currencies could benefit if the financial companies increase liquidity in low liquidity markets, nevertheless, this is quite a small opportunity. Ethereum smart contracts provide a wider range of applications. Financial technology organizations would find it easier to adapt to Ethereum as they can carry out additional applications in addition to leveraging the benefits of Bitcoin as blockchain technology.

Quantitative analysis
Several assumptions need to be made in order to assist in compiling a quantitative analysis to assist in a five-year prediction for each of the cryptocurrency. A total of 100 simulations (Monte Carlo) are run in order to compile an expected return on each currency after five years. Bitcoin outperformed Ethereum in 58 out of 100 simulations. This was largely because of high variance of outcomes for Ethereum large range of factor probabilities as a result of less focused potential use case.

Investment strategy
To consider the various analyses that we performed giving a weighting to every analysis and thereafter use this weighting to allocate the funds of the crypto portfolio. The result of the regression analysis are very positive, although we largely need to discount its result in the overall portfolio decision due to its limitations and has been given only 5% weight. As a result of the nature of the Monte Carlo analysis and it being able to incorporate a number of factors that have a potential to play out over the next five years; the remaining weight has been allocated to the result of this analysis.

In addition, to increase severity, we have introduced three different sub-criteria for the result of the analysis. The first one is the comparison of each 100 simulations, which were produced to determine which blockchain technology had a higher expectation in returns. As this result shows which currency has a higher chance of return over the five-year period, a 40% weight is given in this section. To incorporate the element of risk aversion in making investment decisions, the element of investment criteria was given 25% weight. And finally, there is ensuring that the portfolio will generate a healthy expected result to enable averaging of all the expected returns to produce a probable expected return for the duration of the investment. The final result of this evaluation is given a 30% weight. The following table gives the impact of every weightings had on the portfolio.

The results indicates that Bitcoin is a better performer, nevertheless, Ethereum has proven that it warrants a position in the portfolio. After considering everything, investing 69% in Bitcoin and 31% in Ethereum so as to maximize returns in the next five years. Following this allocation, then we can have an expected value for this portfolio after five years as;
(1.42*0.69) + (1.20*0.31)* $1 million = $1,351,800

**In a nutshell**

With the arrival of blockchain technology as it is, forecasting a five-year increase in the value of either Ethereum or Bitcoin needs a lot of factors to be considered. By combining linear regression, qualitative research through interviews with industry experts and Monte Carlo analysis, we can make a conclusion that Ethereum having a lower expected value has a greater variance due to strong correlation with hype, news and speculation. Ethereum having a great span of outcomes, shows that it should be included in the investment portfolio in order to take advantage of this fact. On the other hand, Bitcoin can leverage its existing user base and is very likely to experience much growth in five years’ time.

**Trading With Monero**

Monero has experienced a thrust with the recent adoption by Oasis darknet markets and Alphabay. This has resulted in price explosion. Monero is the market preferred anonymity focused cryptocurrency. The rise of Monero has rather been slow until August 2016 when it started to rise. It has endlessly competed fueled by speculation and hype rather than utility and innovation. The developers and community of Monero focused on the upgrading and perfecting code to guarantee reliable anonymity.

They paid little attention to cosmetic factors. This resulted to Monero remaining undervalued and unnoticed. Overshadowed by ethically unquestionable and less technically impressive cryptocurrencies. Across social media, forums and other venues of the same where coins received pumping, Monero was hardly mentioned and was severally dismissed as a boring coin.

Through the merits of its code, it won the trust of many people. It has gradually acquired the reputation for competence and reliability. Monero is distinct from the majority of altcoins as it was not cloned from Bitcoin codebase. Monero was introduced as a folk of Bytecoin. The anonymity properties of Monero makes it an excellent choice for darknet market trade and other privacy-sensitive applications.

Monero’s price surge and bust and broader market recognition was as a result of it hitting a couple of darknet markets. The acceptance of Monero by such large markets was not a big deal; rather it reflects a growing trust among those whose freedom rely upon anonymity. For someone who is entirely new in cryptocurrency, there is a lot to learn before making any major investment into Monero. Start with cryptographic techniques that underpin Bitcoin and study the functions of its blockchain. Do not skip the Bitcoin learning part, despite the fact that your main interest is Monero. With no reference to Bitcoin, you cannot be able to properly, predict the relative weakness and strength of Monero.
Chapter 10: Tips For Mining Crypto Currency

When it comes to mining, many find it hard to comprehend the few steps some of which I have clearly and deeply highlighted in this book. With the vast information out there, you can find extra ideas to make your mining process more effective and productive. In this chapter, I will be glad to share with you some of the tricks and tip that you can apply to ease your crypto mining process.

Tips

A mining Rig will be the first order of the business

As far as the process goes, the mining rig is one of the most competitive you will ever see. Most people in this world find it easy and worth to invest in the mining process, numbers of miners coming up with the latest mining software increase every day. With this in mind, you will want to start with due diligence if you hope to have opportunities in this lucrative field.

Cryptocurrency calculator is a device that can help you with research part. All you got do is enter your important information into the coins miner you are planning on obtaining and see how long you will need to make a profit. To be sincere with you, if you do not have at least a couple hundred of dollars to spend you probably will not make it to any big payoffs.
Once you have completed all your necessary calculations, you can then select your miner. If you are not sure which is the best option for you, you can visit mining websites that have reviewed the best option for you. The newest and most powerful option today is the Antminer S9.

Those interested in this should know that things have changed since the early days of crypto mining when it was possible to perform this action from your computer with a graphics card. This was called GPU mining and is no longer an option; today you will need an ASIC miner, which is a specially built computer to handle this task.

**Get a Coin wallet**

Different digital currency may have specific wallet designed for them. Before you even go further, you will need to get a good wallet and ensure the passwords are secure. You will need a place to hold your valuable coins. The wallet is now very easy to get but important to manage properly. Once you have your cryptocurrency wallet you will need to obtain the address; the process has been explained in detail in part of this book.

In case you decide to use a self-hosted wallet, which is a program downloaded onto your computer as opposed to an online service, you will have another crucial step to make. What you will need is a copy of your wallet .dat file stored somewhere safe like on a thumb drive. The reason you will need this is in the event your computer crashes. Without a copy of your wallet.dat file, you could lose all your collected coins. They will not go to another person; they just vanish like burning paper money.

**Get a good mining pool**

Find yourself a good mining pool; there are many advantages when you join a pool. A mining pool is like a group of crypto miners that combine their collected computation
power to produce even more coins at a go. In the mining pool, you will be given an easier algorithm to work on and the combination of efforts will make it quite possible to solve the larger algorithms and earn the block of cryptocurrency that will be divided among the team of miners. This makes the advent of obtaining the coins block a more frequent; you will be making your personal ROIS much faster because you will be working in combination with other miners.

Properly selecting your Mining Pool will require asking some important questions:

What is the reward method? You will want to know if rewards are proportional, PPLNS or score based.

What is the mining fee and charge withdrawing funds?

How frequently are blocks uncovered?

How easy is the withdrawal process?

What kind of stats does this pool provide?

How stable is this pool?

**Have a computer-mining program**

Having the basics, you can begin mining, but you will need a mining client that will handle the operations of your rig from your personal computer. This will help in effective monitoring of your rig. The software you chose will be specific to the mining rig you selected. Many of this mining rig has their own mining software be careful when installing one.

**Organize a VPS**

Having a VPS will make the whole process of mining coins a lot easier and more secure. A VPS will allow a far greater degree of privacy when using digital currency, and quality offerings such as liberty VPS are better, secure and can run anonymously.

**Tricks**

**Choose right GPU**

There are mainly just two GPUs - AMD and NVidia. Go for AMD. Now while choosing AMD, you will see same modes coming straight from Sapphire and from others like XFX Gigabyte MSI. Always try to go for Sapphire originals and never go for MSI.

**Drivers**

For 280-290, cards go with 15.12 drivers. For new cards, go with the newest driver and their new thinge called Radeon Chill.
System
While I know most people love Linux. Windows is king for mining. That is because the best miners are made and updated the fastest on windows. Running them is also very easy - mostly click and play. Currently, Claymore makes best miners, and there was no ZEC Linux version of this at all. Go for Windows.

Make rig at least 5 GPUs
You spent money on parts, and now you want to mine with 3-4 cards? Doesn’t make any sense. Add at least one or two cards.

Windows 7 it will see just 4 cards. Here is a driver that lets you have as many cards as you wish for the system. DOWNLOAD

Windows 10 sees all GPUs right away but uses a little more of resources, so it is better to run Window 7.

Use USB risers
Risers are things connecting your computer with the GPU. Currently, technology went ahead, and it is better to use USB ones. They are more efficient and stable.

Cool down old GPUs
This trick I learned from steemymit1 and it’s brilliant. Used properly will keep your cards alive forever!

Once a year unscrew four screws from GPU, clean this rectangle of old paste and put new thermal paste on it.

Above you can see my AMD 280x and the old paste on it.

Edit virtual memory
Windows had odd virtual memory, and while running few cards on your rig, you have to edit it to 16 GB.

Just go to: Computer Properties -> Advanced System Settings -> Performance -> Advanced -> Virtual Memory
Chapter 11: Strategic Plan in Mining

Cryptocurrency mining is not a casual undertaking. The idea seems simple, but the practice of mining will require handwork. You need to invest a significant amount of money for a startup; you should also be willing to upgrade your equipment’s regularly and constantly monitor the conditions of the coins in the markets. The strategic plans that you need in order to maximize on profits is what I will discuss in this chapter.

**Hardware Requirement**

For the mining process to be a success, there are important parts of the hardware that you must have before you start to mine. The current mining process requires mining power that is processed using the graphics card. The GPU performs faster in solving the algorithms and ensuring that you receive the coins in a short period of time. GPU should be your main mining focus. You can easily get to compare different GPUs performance in this [link](#). You will find the most accurate and current listing for GPU hash rates. When you are mining the same values that apply to litecoin mining, apply to any SHA-256 coin mining.

The following three parts should be considered when building a mining rig

**Graphics card:** For the mining to be a success, graphics card should be of good quality.
**Power supply:** you will need adequate power supply to run your mining setup. If you are getting two or more graphics cards, more power will be required; I would recommend 1000w + power supply.

**Motherboard:** look at the amount of PCI-E slots; this is usually the places for your video cards. You can expand it.

I will give you the basic outline budget for your hardware setup. This setup will get you anywhere between 1000-1200kh/s when mining scrypt coins and 950-1150MH/s when mining SHA-256 coins.

Motherboard: ASRock 970 Extreme3 – $120-$150

Power Supply: SeaSonic X Series X-850 – $175-$200

Video Card: ATI Radeon HD 7950 (x2) – $200-$300/each

Processor: AMD Sempron 145 Processor – $40-$50

RAM: 8 GB Corsair DDR3 – $40-$60

Hard Drive: WD 500GB – $50-$60

Total Cost: $825 – $1120

**The software requirements**

Once you have your computer all setup in place, there are four basics you need to start mining

- updated software and drivers for your video cards
- mining software
- coin wallet
- Internal connection

**Operating system updates**

Ensure that your operating system has all the latest updates. This will help in minimizing the risk of security breaches and hacking.
Graphics cards software and drivers
The most important part of getting your mining ready is to update and download the latest software for your video card. You can download the latest version from the following links.

ATI SDK’s from [here](#) and ATI drivers from [here](#)

Download the software and install them on your machine using the default settings.

Mining software
The best mining software to use currently is the CGminer. It has been proven stable and has provided exemplary work. Below are the links to their specific download locations.

- CGMiner
- Poclbm
- Phoenix Miner (Linux)
- DiabloMiner (MAC OSX)

Coin wallet
Download specific coins wallet for a successful mining. In case you want solo mining, you will need to download specific coins wallet. This will act as a local mining client on your machine. However, I would recommend someone not solo mine heavy coins like bitcoin and litecoins. Their difficulties are too high, and it would take an incredibly long time to actually mine a single block chain.

Configuring your miner
Assuming you are using CGMiner and have installed it to the C: CGMiner directory, all you need is to just launch the application as I have explained in the previous chapters through a command line.

The basic information you will need to launch CGMiner is the following:

- `o *servername:port*`
- `-u *yourusername*`
- `-p *yourpassword*`

To launch your miner, you would simply click Start > Run and type in: "C:\CGMiner\cgminer.exe -o servername:port -u **yourusername** -p **yourpassword**" (without the **). This is the basic command to mine a SHA-256 coin (i.e. Bitcoin)
If you want to mine a Scrypt based coin, you simply need to add the “–scrypt” flag after you call cgminer. Therefore, your command would look like this:

C:\CGMiner\cgminer.exe --scrypt -o servername:port -u **yourusername** -p **yourpassword**

If you solo mine, your server name will be the local IP address for your computer and the port will be the same rpcport you had set in the configuration file, which will need to be set as the following

C:\CGMiner\cgminer.exe --scrypt -o 127.0.0.1:7998 -u YourUsername -p YourPassword

If you want to make things easier, create a simple text file on your desktop and paste the above command in the file. Save the file as a .bat or .cmd file (Ex: MineDigitalcoin.bat). Then, to start mining double click on your batch file and the command will execute.

**Optimization**

At this stage, you will have been running your mining setup and actually receiving the coins. However, you will notice that your results are lower than for the others. This is because your rig setup is not optimized. Graphics card can be overclocked and underclocked to achieve optimal results.

Overclocking and underclocking your hardware beyond factory settings may sometimes harm your hardware and make your mining void.

**Video card optimization**

When you overclock your graphics cards, it can lead to a significant performance increase. When you are using the ATI software, you can download Trixx or MSI afterburner to tweak your software’s settings. The three main settings that you will need to adjust are your core speeds, your memory clock speeds, and your voltage. For best results, you will keep your memory clocked about a third higher than your core speed, and you will set your voltage slightly lower than the default.

**CGMiner optimization**

You can also launch sgminer with the optimized settings in the command line. The switches for cgminer are:

Another thing you will want to set in your CGMiner is a target temperature and your fan. Generally, for most cards, we suggest automatic fan setting and a target temperature of up to 80°C. The switches for these settings are:

--temp-target 80 --auto-fan

Finally, use your CGMiner to set up a backup pool in case your main pool goes down. Find a second pool for the same type of coin (SHA-256 or Scrypt) and sign up for it. You can then set up your pool as a failover pool in case your main one goes down. The command to add to CGMiner for this is:

--failover-only -o backup-pool-address.com:portnumber -u user -p password

Simply fill in the pool address and port and the username and password you created.

Your entire command should look as follows:

cgminer --scrypt -I 18 -g 1 -w 128 --thread-concurrency 21712 --gpu-engine 1050 --gpu-memclock 1400 --gpu-vddc 1.087 --temp-target 80 --auto-fan -o mail-pool-address.com:portnumber -u user -p password --failover-only -o backup-pool-address.com:portnumber -u user -p password

Now, in your batch file to launch CGMiner, simply add the following lines at the very beginning:

Timeout /t 30

setx GPU_MAX_ALLOC_PERCENT 100

setx GPU_USE_SYNC_OBJECTS 1

Your final batch file should look like this:

Timeout /t 30

setx GPU_MAX_ALLOC_PERCENT 100

setx GPU_USE_SYNC_OBJECTS 1

C:\CGMiner\cgminer.exe --scrypt -I 18 -g 1 -w 128 --thread-concurrency 21712 --gpu-engine 1050 --gpu-memclock 1400 --gpu-vddc 1.087 --temp-target 80 --auto-
fan -o mail-pool-address.com:portnumber -u user -p password --failover-only -o backup-pool-address.com:portnumber -u user -p password

**Computer optimization**

The final thing that you need to do to have a successful mining is to optimize your computer and its operating system. This involves disabling unused services, changing your power settings and setting your computer to automatically power on the start of mining process in case of a power outage.

The first things you will want to look at are your BIOS settings. When you start your computer, enter the BIOS setup, and look at the power options. This is important because when your computer is off, you are not mining, and if you are not at home when the power turns back on, your computer will stay off until you manually turn it back on. Setting this option will ensure that as long as there is power, your computer will be on.

Next, you will configure the computer to automatically log in. If there is no power and your computer restart, you need not to be stuck on the log in screen. Just click Start > Run and type “netplwiz”. Then, uncheck the box “Users must enter a user name and password to use this computer.”

Following these steps will ensure that you are able to mine at the highest rate possible. The process also ensures that you can mine even when the main pool goes down. Therefore, a downtime will only be experienced when there is absolutely no physical current going to your rig. Therefore, as soon as power is restored to the house, the computer will turn on and restart mining.
Chapter 12: Conclusion

Enthusiasts, investors, consumers, or even tech-savvy geeks may be good Bitcoin buffs. All this type of people may follow every bit of cryptocurrency news and have one question in their mind. Individuals may want to find out if the optimistic future can be carved out of mining different cryptocurrencies. Well, it is not a startling or gimmick infomercial. Cryptocurrency mining can be an intelligent attempt, apart from being lucrative. The latest popularity of Cryptocurrency market can’t be denied. The boom of bitcoin in 2013 together with its enormous increase in value resulted to its reputation. The rolled costar ride of cryptocurrencies known as Altcoins and Bitcoin got a place of distinction in each dictionary found in the world. These digital currencies over the years have earned sufficient exposure, and a career involved in mining them can provide income. However, the miners should have three main things – some money, ample time, and an undying perseverance.

Selection of a cryptocurrency to mine is the first hurdle. As a miner, you can start mining Bitcoin. You can as well settle on other altcoins we have talked about in this book. In simple terms, you have a lot of options. Just like stock, cryptocurrencies also have categories, penny or blue chip. Blue chip mining is mostly associated with reliability, safety, and bigger profit. Banking on this features, individuals are more persuaded towards mining Bitcoin, even if it involves using a heavy computing power. On the other hand, other cryptocurrencies can also provide a good gain since
its algorithms are simpler. However, with Altcoins, the potential gains and simplicity of mining are not necessarily proportional.

The real test begins to be revealed through the hardware. Even techno-savvy miners can’t deny the Bitcoin difficulty which is linked to a new block generation. At this point, one is found in a dilemma to decide which computing power should be utilized. For Cryptocurrency like Bitcoins, their algorithms have turned from difficult to hash. Hence, GPU of colossal power coupled with reliable hard disk drives and high-end RAMs have to do all the tasks. The whole point is to hash at a swift rate.

Several high-end GPUs that run together can accelerate block generation and subsequently the payouts. However, the right piece of software may not be as tricky. Someone can choose Windows as the needed Operating System, although open-source Linux does a greater job. The digital wallet is another. Mined digital currencies need to be stored. As a miner, you can store it remotely online or locally on your hard-drive. You just need to choose smartly.

Once you have the software and hardware in place, the mining task can start. A miner may be able to do it alone and collect all benefits. Although your rig needs to be extremely powerful. Therefore it is quite implausible. A viable solution is mining in pools since several people team up to provide hash machines and power. Thus digital coins get mined at increased velocity. Working as a team has its own advantages; miners acquire their fair share. Multi-pool mining is an inexpensive alternative. If cryptocurrencies mining is to be undertaken, Middle-coin should be the choice of the miner. So with all the necessary tools in place, a profitable mining rig can start. Initial investment might seem overwhelming, but the benefits are worthwhile!