Gain insights into Bitcoin, a cryptocurrency and a powerful technology, to optimize your Bitcoin mining techniques

Bitcoin Essentials
Albert Szmigielski

Blockchain is being billed as the technology of the future. Bitcoin is the first application of that technology. Mining is what makes it all possible. Exploring mining from a practical perspective will help you make informed decisions about your mining setup. This practical guide starts with an introduction to Bitcoin wallets, as well as mining hardware and software. You will move on to learning about different mining techniques using the CPU, GPU, FPGA, and ultimately the ASIC as an example. After this, you will gain an insight into solo mining and pool mining, and see the differences between the two. The book will then walk you through large-scale mining and the challenges faced during such operations. Finally, you will take a look into the future where blockchain-based applications are common and mining is ubiquitous.

Who this book is written for
If you have never mined before, this book will ensure that you know what mining is all about. If you are familiar with Bitcoin mining, then it will help you to optimize your mining operations. A basic understanding of computers and operating systems is assumed, and some familiarity with cryptocurrency basics would be an added advantage.

What you will learn from this book
- Get introduced to Bitcoin mining from the ground up
- Find out about mining software and the different types of mining hardware
- Master setup techniques to enable efficient mining
- Examine the pros and cons of the different types of mining hardware
- Deduce the differences between solo and pool mining
- Take a peek into professional mining farms
- Explore the future of mining and blockchain-based applications
In this package, you will find:

- The author biography
- A preview chapter from the book, Chapter 1 'Bitcoin Wallets and Mining Software'
- A synopsis of the book’s content
- More information on Bitcoin Essentials
About the Author

Albert Szmigielski is a thinker, a computing scientist, a software engineer, and a blockchain professional. He holds a BSc in Computer Science and an MSc in Digital Currency. He has been involved in a number of start-ups and software projects. He believes in a decentralized, distributed nature of storing information, and hence has an interest in Bitcoin and blockchain technology.

Albert is a researcher at CryptoIQ and a mentor at the Blockchain Institute. He frequently contributes to his blog at blog.cryptoIQ.ca.
Surely, by now you have heard of the phenomenon called Bitcoin. Is it digital money, is it a payment system, is it a network, or is it something else? The answer is yes to all the previous questions. Bitcoin is all of those and more. In this book, we will concentrate on the mining aspect of Bitcoin. Mining is how new bitcoins are created and how transactions are accepted into the Bitcoin blockchain. We will show you how to mine for yourself, if you are interested. We explain step-by-step what is necessary and how to do it. CPU, GPU, FPGA, and ASIC mining is also discussed. We will examine solo mining and pool mining. We will spend a little bit of time taking a look at large mining operations. Finally, we will speculate what the future may look like in the mining world of Bitcoin.

What this book covers

Chapter 1, *Bitcoin Wallets and Mining Software*, gives an overview of Bitcoin wallets: hardware, software, full and thin clients. The chapter also discusses mining software.

Chapter 2, *CPU Mining*, looks at Bitcoin mining using a CPU. It covers everything you need to get started.

Chapter 3, *GPU Mining*, concentrates on GPU mining. It covers GPU driver setup, mining software setup, and it touches upon practical mining issues. Examples are included.

Chapter 4, *FPGA Mining*, examines FPGA mining, including software, drivers, and a discussion of best practices.

Chapter 5, *ASIC Mining*, looks at ASIC mining in detail. We set up the software that is needed to mine and we show you practical examples of mining with ASICS.

Chapter 6, *Solo Versus Pool Mining*, explains solo and pool mining and weighs the pros and cons of both ways of mining.
Chapter 7, Large Scale Mining, looks at mining as a business. There are a handful of companies that decided to mine for profit. They represent the bleeding edge in mining techniques.

Chapter 8, The Future of Bitcoin Mining, speculates how mining may evolve in the future. We look at the possibility of mining becoming more centralized and the possibility of mining becoming decentralized.
In this chapter, we will take a look at the various Bitcoin wallets available, explore the mining software that is currently available, review the functions that Bitcoin wallets perform, and why we need them. We will take a brief look at both software and hardware wallets. The difference between full wallets and thin client wallets will also be explored. We will also touch upon hosted wallets and look into wallet security.

Next, we will take a brief look at mining software and examine why the software is needed and what it does. Finally, we will quickly review what mining software is available to us and which software we should use. Keep in mind that the material presented in this chapter will be brief and serve only as a review of the basics:

- Bitcoin wallets
- Types of wallets
- Wallet security
- Mining software

**Bitcoin wallets**
In this section, we will take a closer look at Bitcoin wallets. We will define what a wallet is and explain why we need a wallet. We will look at the types of wallets available. There are software and hardware wallets, full wallets, and the so-called thin wallets. There are also hosted wallets that are run by companies for the users' convenience. We will look at the most popular wallet called **Bitcoin Core**; finally, we will touch upon wallet security.
What is a Bitcoin wallet?
A Bitcoin wallet (sometimes called a client) is a software that facilitates performing bitcoin transactions. Wallets come in different flavors. The most capable of them are called full clients. They can perform bitcoin transactions and act as a gateway to the Bitcoin network. Full clients also store a copy of the Bitcoin block chain locally. An example of a full client is the Bitcoin Core software application.

Definition

Block chain: The Bitcoin database that stores all the transaction data is called a block chain. The transactions are grouped together in batches for efficiency reasons. A batch is called a block and each block (except for the first, called genesis block) has a link to the previous block. This linking together of blocks is the chain part of the block chain.

A wallet allows us to send (spend) and receive bitcoins. These are the main transactions that most users will perform. Most importantly, a wallet stores your secret private keys, so that you can access the bitcoins you own. The name "wallet" is slightly misleading. The wallet actually does not store bitcoins directly. All the bitcoins are stored on the block chain and the wallet software simply allows you to transact with the bitcoins that the private keys stored in the wallet have control over. In simpler terms, wallets store private keys. Those keys are tied to bitcoins on the block chain and therefore you can send them to another address.

A wallet also allows us to look into the Bitcoin network and see additional details. It allows us to see information about the Bitcoin network, the block chain, mining, and the wallet in general. We will go over these in later chapters.

Why do we need Bitcoin wallets?
As mentioned earlier, wallets facilitate Bitcoin transactions. Without them, moving bitcoins from one address to another would be impossible. It is worth noting that a wallet is a fundamental piece of Bitcoin software. A wallet is the required software in order for the Bitcoin network to exist.

Without the ability to transfer bitcoins, the system would not be very useful. In the original wallet called bitcoin, the transactions had to be put together manually. Later on, the wallet software was expanded and updated to make transaction creation seem like a breeze. Since wallets connect us to the Bitcoin network, they are also needed in mining operations. While mining, it is the wallet software that communicates with the Bitcoin network. It watches out for new blocks, so that if a new block is found by some other participant, our mining software can stop working on the now solved block and move on to the next.
The transactions that our mining software will put in a candidate block also come from the wallet. In addition, wallets verify found blocks and propagate transactions that come onto the network.

**Types of wallets**

Wallets have come a long way since the original came out in 2009. There are now software wallets, hardware wallets, paper wallets, hosted wallets, and, of course, there are innovative companies who constantly think up new ways to create wallets.

**Software wallets**

There are a variety of software wallets. For an up-to-date list of the most popular wallets, see [https://bitcoin.org/en/choose-your-wallet](https://bitcoin.org/en/choose-your-wallet). We will concentrate here on the Bitcoin Core software application. At the time of writing this book, the current version is 0.11.2. You can always check the latest version here: [https://bitcoin.org/en/download](https://bitcoin.org/en/download).

If you do not have Bitcoin Core installed and you would like to mine solo (solo mining will be explained in *Chapter 6, Solo Versus Pool Mining*), it would be a good idea to download and install it. Make sure that you have sufficient space on your hard drive for the block chain, which currently (Feb 2016) is about 55 GB. Once you install Bitcoin Core, it will proceed to download the block chain, which may take a while. When you open the software, you will be greeted with the following screen:

![Fig. 1.1: The Bitcoin Core wallet.](image)
As you can see, the client is downloading the block chain by synchronizing with the Bitcoin network. There are tabs to send and receive bitcoins. There is also a **Transactions** tab, under which you can find a history of all transactions performed with the wallet.

![](Fig_1_2发送.png)

**Fig. 1.2**: Send tab in the Bitcoin Core wallet.

The **Send** tab can be used to transfer the bitcoins you control to another address. It requires a destination Bitcoin address and the amount you wish to transfer. If your wallet is password-protected (more on securing your wallet later), you will be prompted to enter it.
The **Receive** screen, on entering the relevant information and pressing **Request payment**, will generate a QR code and a URI that can be sent out or posted online.
The Transactions tab lists all the transactions tied to the private keys that the wallet is storing.

The functions described in the preceding section are the basic wallet transaction types, but what is more interesting is the information we can get about the network through the Bitcoin console. The console can be accessed by going to the Help menu and selecting Debug window.

---

**Fig. 1.5: The Transactions tab in Bitcoin Core**

**Fig. 1.6: Debug window of Bitcoin Core**
Select the **Console** tab and you will be able to obtain a trove of information about the Bitcoin network and about Bitcoin's block chain. To see a list of possible commands, type `help` into the console and press *Enter*. You will be presented with a long list of commands that have been grouped in categories. A complete overview of the commands is beyond the scope of this book. However, we will take a look at some of them.
Bitcoin Wallets and Mining Software
Fig. 1.7: A listing of all available commands

```
== Wallet ==
addmultisigaddress nrequired ["key",...] ["account"]
backupwallet "destination"
dumpprivkey "bitcoinaddress"
dumpwallet "filename"
getaccount "bitcoinaddress"
getaccountaddress "account"
getaddressesbyaccount "account"
getbalance ("account" minconf includeWatchonly)
getnewaddress ("account")
getrawchangebyaddress
getreceivedbyaccount "account" [minconf]
getreceivedbyaddress "bitcoinaddress" [minconf]
gettransaction "txid" [includeWatchonly]
getunconfirmedbalance
getwalletinfo
importaddress "address" ["label" rescans]
importprivkey "bitcoinprivkey" ["label" rescans]
importwallet "filename"
keypoolrefill ["newsize"]
listaccounts [minconf includeWatchonly]
listaddressgroupings
listlockunspent
listreceivedbyaccount [minconf includeempty includeWatchonly]
listreceivedbyaddress [minconf includeempty includeWatchonly]
listsinceblock ["blockhash" target-confirmations includeWatchonly]
listtransactions ["account" count from includeWatchonly]
listunspent [minconf maxconf ["address",...]]
lockunspent unlock ["txid","txid","vout":n,...]
move "fromaccount" "toaccount" amount [minconf "comment"]
sendfrom "fromaccount" "tobitcoinaddress" amount [minconf "comment"
"comment-to"]
sendmany ["fromaccount" ["address":amount,...] [minconf "comment"
"address",...]]
sendtoaddress "bitcoinaddress" amount ["comment" "comment-to"
subtractfeefromamount]
setaccount "bitcoinaddress" "account"
settxfee amount
signmessage "bitcoinaddress" "message"
updatelock
walletpassphrase "passphrase" timeout
walletpassphrasechange "oldpassphrase" "newpassphrase"
```
Perhaps, the most interesting to us will be the `getmininginfo` command. Typing it into the console yields the following:

![Debug window with getmininginfo output]

As we can see, the command returns the last block number, current mining difficulty, network hashing speed, and some other information as well. There are websites that check this information for each block and offer graphs to visualize the data. They are called block explorers and there are many of them. The most popular perhaps is [http://blockchain.info](http://blockchain.info).
You can find out more information about any command by typing `help` followed by the command name. For example, to find out more about the `getmininginfo` command, we will type `help getmininginfo`:

![Debug window](image)

Fig. 1.9: Getting more information about a command: `help getmininginfo`
Another interesting command from a mining point of view is the `getblockchaininfo` command. The following screenshot shows us the output and the help data on that command:

![Fig. 1.10: Output of the getblockchain info command and help getblockchain info](image)

**Hardware wallets**

Hardware wallets are a relatively new addition to the array of Bitcoin wallets available. They are not required for mining purposes, but are great for keeping your bitcoins safe. The two most popular solutions on the market are Trezor and Ledger wallets. We encourage you to take a look at their respective websites, if you think you can benefit from a hardware wallet.
The major advantage of hardware wallets over software ones is their security. They are not affected by computer viruses designed to attack software wallets. They are offline for a majority of the time (online only to compose a transaction). They also enjoy an advantage over paper wallets, as a result of being interactive versus importing the whole wallet, as in the case of a paper wallet.

**Full wallet versus thin client**

Any wallet that stores the entire block chain database is regarded as a full wallet, Bitcoin Core is one example. Sometimes there just aren't enough resources available to download and store the complete block chain. This could be due to bandwidth restrictions, storage limitations, or perhaps just an unwillingness to run the full wallet.

There are wallets available that do not download the entire block chain. This is obviously required for mobile computers with limited storage, such as smart phones and tablets and other Internet-of-things devices. These types of wallets are called thin clients. They use a procedure called Simplified Payment Verification (SPV) to avoid having a full copy of the block chain. SPV is not important for mining purposes, but every miner should at least know that the security of an SPV wallet is not as tight as the security of a full wallet.

**Hosted wallets**

There are a number of companies that offer hosted wallet services. This means that you do not need to download or install any software and of course downloading the block chain is also not required. There is a trade-off when you use a hosted wallet. You are giving away a part of the security that comes with running your own wallet in exchange for convenience.

However, as these hosted wallet companies are maturing and becoming big, their ways of securing bitcoins may be better than that of a single user. The risk of insolvency is then the biggest risk to a hosted wallet user. If the company goes bankrupt, then the funds stored in their hosted wallets will most likely not be recoverable. Just like with a traditional bank, deposits are liabilities of the bank and in the case of failure, depositors would only be able to recover the portion of their deposits that is insured by the government. We are not aware of any such insurance schemes available to hosted wallet providers.
Wallet security
Securing your wallet is a serious matter. With Bitcoin being deflationary, the value of the cryptocurrency is expected to rise in the long term. Therefore, making sure that your funds are only accessible to you is a worthwhile undertaking. Your online wallet should be encrypted and password-protected. Furthermore, you should back-up your password protected wallet to multiple locations.

To encrypt your wallet, select Encrypt Wallet from the Settings menu in Bitcoin Core and then follow the rest of the instructions. Please remember to choose a very strong password.

Make sure to use upper- and lower-case characters; also add some special characters and make the password long (min. 10 characters). It is also possible to make a passphrase out of ten (or more) random words. It will be beneficial if those words are not in a dictionary (use misspellings or combination words). Finally, it is a good idea to only keep a small amount of bitcoins in your online wallet. The bulk of your holdings should be kept offline. A full discussion of securing your wallet is impossible here. We do encourage you to find resources online to educate yourself more about this topic.

Mining software
Let’s now look at mining software. At the very beginning, mining software was built into the wallet software. Mining used only a single core of a CPU back then. Nowadays, there are a variety of devices that can perform the mining function. As such, there is some software needed to coordinate and manage the work done by these devices.

The need for mining software
As mentioned earlier, mining software coordinates and manages the work of different mining devices. In order for mining to move beyond utilizing a single core of a CPU, software was needed that could manage the work that multiple cores perform. This is to make sure that they do not do redundant work; hence, mining software was born. Later on, mining moved onto a multitude of devices and the need for a management software became even more apparent.
What does mining software do?

Bitcoin mining is basically a guessing game. The software constructs a candidate block. A candidate block includes the hash of the previous (last) block and it also includes transactions taken from the pending transaction pool. Finally, it includes the most important piece, called a nonce. A nonce is basically a counter. The software constructs the candidate block and then hashes it. If the result does not meet the difficulty criteria, then the nonce is incremented and another hash is taken.

Mining devices can make billions and even trillions of these hashes per second. When a successful hash is found, the software submits the solved block to the network for verification. We call this guessing rather than solving because solving implies a method other than repeated guessing and checking if it is correct.

Which mining software to choose?

There are a variety of different software miners. A good comprehensive list can be found at: https://en.bitcoin.it/wiki/Mining_software. The two most popular miners are cgminer and bfgminer; both are open source and can be downloaded from GitHub. Here, we will concentrate on cgminer.

Cgminer can be downloaded from a variety of sources on the Internet. We recommend going directly to the developer's website: http://ck.kolivas.org/apps/cgminer/.

Cgminer is available for Windows and Linux systems and it can also be built from source for Mac OS; there are also third party providers that host a compiled Mac OS version on their websites. Download the appropriate version for your system. Installation on Windows systems is straightforward. As an example, we are going to use cgminer version 3.7.2. This is the last version to support GPU mining; keep this in mind if you want to mine with your GPUs. (We will further discuss the versions of cgminer in the chapters on mining with specific devices.)

**Definition**

**GPU**: Graphics Processing Unit is a processor designed specifically for processing and displaying graphics on a computer screen.
Once you have cgminer installed, you may want to verify it by running the cgminer -n command in your terminal (also called command prompt in Windows). The output will look similar to this:

It lists the required software (OpenCL in our case) and confirms that cgminer found some hardware in your system that it can use to mine. In our case, it is an AMD R9 Radeon GPU.

Now would be a good time to start cgminer and familiarize ourselves with the basic features. In order to run cgminer, we need to tell it where to get work from. This means a mining pool or your local wallet if you are mining solo (more on this will follow in the chapters on mining solo or with a pool).

**Definition**

**Mining pool**: Bitcoin mining is very competitive and in order to have a better chance at being successful, individual miners combine their resources together and form groups, also called pools. Such a combined mining group is called a mining pool. A quick Internet search will show that there are a number of mining pools out there.

If you are already registered with a pool, run the following command to start mining:

cgminer -o <http://pool:port> -u <username> -p <password>

This tells cgminer to connect to the specified pool with the specified credentials (of course, replace the values in the angle brackets with your own pool information).
If successful, cgminer will start and display the following screen:

![cgminer output]

As we can see, cgminer is running and it is connected to the pool we specified.

We will now briefly review the options that cgminer offers while it's running.
There are menu items for: **Pool management**, **GPU management**, **Settings**, and **Display options**. Let’s examine them a little more closely. To get into a menu item, simply press the letter that corresponds to the item in question. The letters are wrapped in square brackets to indicate that they can be selected.

The following is the screenshot of **Pool management**:

![Command Prompt - cgminer](image)

Fig. 1.13: Pool management in cgminer
Here we can add more pools, remove ones we no longer need, disable, enable pools, or change the mining quota. We can also change our management strategy.

As we can see, there are five options for pool management. We usually use the default option: Failover, which switches to the next pool in the case of the current pool's outage. These options are best explained in the README file that is included with cgminer.
The next option is **GPU management**—pressing G will bring up the following screen:

![GPU management screen](image)

Fig. 1.15: GPU management screen

Here we can see the current statistics about our GPUs. The read-out shows temperature, fan speed, GPU clock, memory clock, and other information that maybe available for the particular hardware at hand. We can also manage our GPUs, in case we have multiple ones. We can disable or enable additional GPUs, change the intensity setting on each GPU, and change other settings as well.
Let's exit this menu (press space to exit) and go back to the main screen. Let's now look at the **Settings** menu. Pressing S will bring up the following screen:

![Fig. 1.16: Settings options in cgminer](image)

Here, the most interesting option is **Write config file**. Pressing W will save a config file that we can use in the future to start cgminer with the appropriate settings. We will go into details in a later chapter – right now we want you to be aware that such an option exists, as it will prove useful.
Bitcoin Wallets and Mining Software

Finally, the **Display option** from the main screen of cgminer will let us control what we want to see on the screen while cgminer is working. Pressing \( D \) will bring us to the following screen:

![Fig. 1.17: Display options](image)

We find that the default display options are sufficient for most miners. If you are interested in additional details, you may want to delve into the options by reading the **README** file that is shipped with cgminer. We do recommend everyone to at least skim through that file, as it is filled with useful information. We will touch upon the most important functions of the software later on, but a full description and explanation of all the features is beyond the scope of this book.

Finally, we should note that exiting cgminer, for whatever reason, can be accomplished by pressing \( Q \).
Summary

In this chapter, we glanced at Bitcoin wallets and mining software. We examined the different flavors that wallets come in, from software wallets to hardware wallets. We looked at the difference between full wallets—ones that keep a full copy of the block chain, and thin client wallets that do not download the entire block chain but instead use a different technique to verify transactions. We also touched upon hosted wallets and wallet security was covered at a basic level. Always keep in mind that securing your wallet is an activity worth the effort.

Next, we looked at mining software. We discussed why such software is needed and what it accomplishes. We examined mining software by looking at one of the most popular: cgminer. We briefly discussed the options available when running cgminer.

This chapter was meant as a refresher—we will delve deeper into these topics in subsequent chapters. We hope that you found this chapter interesting and will stay with us for the rest of the journey.
Where to buy this book

You can buy Bitcoin Essentials from the Packt Publishing website.

Alternatively, you can buy the book from Amazon, BN.com, Computer Manuals and most internet book retailers.

Click here for ordering and shipping details.