Bitcoin Hands-On!

28 “learn-by-doing” exercises to master the basics of managing your own Bitcoin, including wallets, transactions, and self custody

Sylvia Vasilik

ISBN 978-1-7341663-2-3 (ebook)
ISBN 978-1-7341663-3-0 (paperback)
ISBN 978-1-7341663-4-7 (hardcover)

Published by Fluid Progress Press
Version 218
August 2026

Disclaimer

This book is intended for educational and informational purposes only. The content is the author's understanding of Bitcoin. It should not be considered financial, investment, legal, or tax advice. Always do your own research, consult qualified professionals, and follow local laws and regulations. Protect your private keys and other data—lost or stolen keys mean lost funds.

By reading this book, you accept full responsibility for your actions and acknowledge these risks.

Contents

Introduction

First of all, thank you for purchasing this book! Any feedback would be appreciated. For any questions or issues, please send email to Feedback@BitcoinHandsOn.com.

I'll start out by telling you what this book is not. It's not about the "why" of Bitcoin. I'm going to assume that since you're reading this book, you're convinced that Bitcoin has a lot of promise, and you believe that learning how to use Bitcoin directly, without intermediaries, is important.

It's also not about the history of money, why government currencies (also known as "fiat currencies") seem to inevitably fail, how inflation is actually theft, or similar topics. There are writers much smarter than I am who have gone over these topics, in depth. I list some of the best books in the Resources section, at the end of this book.

Instead, this book is all about actually using Bitcoin. It's about using software to create wallets that you control directly, known as **self custody**. It's about understanding, at a very practical level—what is a private key? And why is it important?

It's about learning to manage your wallets, and sending and receiving sats (short for satoshis, 1 bitcoin equals 100 million sats) without needing to go through gatekeepers like banks or investment firms. Learning how to use Bitcoin may be the most important technical skill you ever develop.

Why is self custody important?

Holding your own bitcoin (self custody) is key to getting the benefit of Bitcoin, over the long run.

If you already own bitcoin, is it in self custody? Well, if you don't have the private key—the private key that you could use to send and receive the bitcoin directly—then it's not in self custody.

Let's look at some cases where people think they own bitcoin, but they don't actually control it:

- If you're holding bitcoin on an ETF (exchange traded fund), then you don't have bitcoin in self custody, it's all managed by the fund. It's not possible to withdraw actual bitcoin from the exchange. Instead, you need to sell the bitcoin and withdraw USD.
- If you're holding bitcoin on an exchange, such as Coinbase or Kraken, then you still don't have bitcoin in self custody.

An exchange is an improvement over an ETF, because usually you can withdraw the bitcoin into a self custody wallet.

But still, many exchanges have failed—through hacks or fraud—since Bitcoin's creation. Early bitcoiners learned through bitter experience that they shouldn't trust exchanges.

The history of Bitcoin exchanges is full of these scams and thefts, ranging from one of the earliest and most famous (Mt. Gox in 2014) to more recent scams (FTX and Celsius in 2022).

There's one thing these disasters had in common. It's that the supposed "owners" of the bitcoin did *not* actually hold their own keys. Instead, they left their bitcoin in the custody of others, in what are called "custodial wallets". People thought it was safer to have their bitcoin in the custody of large firms, instead of managing it themselves. They were wrong.

Not your keys, not your coins

If you didn't understand "*Not your keys, not your coins*", you wouldn't have necessarily known that you were doing something dangerous, by relying on other people to manage your bitcoin.

For instance, take one of the more recent exchange failures, FTX. Mainstream media news coverage of FTX was glowing. It stayed positive until just before the whole thing unraveled, and was revealed as a huge scam. Most users didn't realize they were taking a serious risk by leaving their bitcoin on the platform.

It's not as hard as it seems

For many people, self custody—using bitcoin directly and holding the private key themselves—is intimidating. Without an intermediary like a bitcoin exchange or ETF, people worry about making mistakes and losing their hard-earned money. Many people avoid self custody because they don't understand seed phrases and private keys.

Bitcoin can seem mystifying and complex. It may seem that using Bitcoin requires an understanding of the underlying technology, and in-depth knowledge of cryptography.

But that's absolutely not true. I'm here to tell you that you do *not* need this in-depth knowledge. Do you need to understand how a car engine works, in order to drive? No, you don't. You also don't need to understand every technical detail about how Bitcoin works, in order to safely use it.

Taking small steps in a safe environment

The learn-by-doing exercises in this book will walk you through the process of learning Bitcoin, one simple step at a time.

When you're learning to drive a car, do you immediately start driving on the highway? No, you don't. You head to a large parking lot, and practice driving there. You make a lot of left turns and right turns, starts and stops. That's what you'll be doing in Bitcoin, Hands-On—lots of practice, in a low-risk environment.

Working your way through this book will help you overcome the anxiety that can come with managing your own bitcoin. The exercises use a few temporary, small test wallets, that you create and control. This is the Bitcoin equivalent of taking your first drive in a parking lot, to learn about the steering wheel, gas pedal, and brake.

With these small wallets, you'll make steady progress through the exercises with small amounts, gaining confidence and learning to avoid the problems that can occur. You master the skills you need to safely send, receive, and store bitcoin.

How to get the most out of this book

Here's a few tips on going through the exercises, and how to really learn the practical aspects of Bitcoin—in a way that sticks.

- Name the wallets exactly as shown in the instructions. This makes it easier to follow along, because the same wallets are used throughout the whole book.
- Complete all the exercises, even if you think you know what's going to happen. Actually doing the steps is key to learning. Just reading isn't enough.
- You may want to start Exercise 3 (Buy Bitcoin) first. It can take a few days to set up an account on exchange, so it's good to get the process started. This is because exchanges require identity verification, due to government financial regulations.
- Consider doing each exercise twice. First, follow along step by step with the book. Then, try it again without the instructions—just from memory and the name of the exercise. That's where the real learning happens.
- Transaction fees in recent years have been very low. But if you're concerned about fees, the lowest fees are usually on weekend mornings, US east coast time (EST). So, consider doing the exercises that involve transactions during that time. You'll learn more in exercises 17 and 18 about fees.

Author's note on Bitcoin capitalization:

Standards are still evolving on when Bitcoin should be capitalized, but the consensus seems to be—upper case when speaking of Bitcoin as a system,

and lower case when speaking of the currency units, or as an adjective. That's what I do in this book.

Exercise 1: Install Sparrow Bitcoin Wallet

In this step we'll install Sparrow Bitcoin Wallet. Sparrow is the most widely used and respected desktop Bitcoin wallet. It's free—and more importantly, it's open source.

Open source software means that the code is publicly available for review. You can see the actual Sparrow Wallet source code on the site GitHub, and can read the whole thing. This allows people to verify there's nothing harmful hidden in the software.

Sparrow Wallet is suitable for beginners, but has all the functionality expert users need as well. So, it's a great tool to use on your Bitcoin learning path. The Sparrow version that I used is 2.5.2. However, it's frequently updated, and your version might be different. If any changes significantly impact these exercises, I will update them.

To install Sparrow, go to https://sparrowwallet.com and click the download link at the top. You'll see options for downloading versions for MacOS, Windows, and Linux. Download and install whichever version matches your operating system. The instructions for the install will be different for each operating system.

If you're using Windows, there's an Installer version and a Standalone version. Download the Installer version unless you have a specific reason to use the Standalone version. During the install, leave all the settings at the default.

The instructions in the exercises will be with the Windows version of Sparrow, but it should be very similar in the MacOS and Linux versions.

I get a warning "Windows protected your PC" when I try to install

If you're running Windows, there are filters turned on to protect you against unsafe software. But this filter can also be triggered by software that's less common, like Sparrow. As long as you've downloaded Sparrow

from the above link, you're fine. In the warning window, click "More info" and then "Run anyway" to continue with the installation.

In the Edge Browser, the Sparrow download has an orange warning triangle

When using the Windows Edge Browser, a message comes up saying that the file isn't commonly downloaded, and make sure you trust it before opening it. Click on the 3 dots to the right of this message, click Show more, and then Keep Anyway.

Is it hard to see the full screen in Sparrow, or is the text too small?

Sparrow is written in Java, to make it easier to run on different operating systems. However, one disadvantage is that it can cause screen resolution problems.

On my computer, I just live with it because it's not too bad. But you can also change the resolution by clicking on the Windows Start button, typing "Resolution", and then choosing the option "Change the resolution of the display".

Under "Scale and Layout", click the dropdown under "Change the size of text, apps, and other items". I experimented with reducing my resolution. On your computer you may need to reduce or increase the resolution.

For more details, go to https://sparrowwallet.com/docs/faq.html, and search for the word "resolution".

What server to connect to?

When you install Sparrow, you'll get some options about choosing a server. This server is what Sparrow uses to point to the Bitcoin network. For now, we'll stick to the default of using a public server, mempool.space.

Troubleshooting your connection in Sparrow

Occasionally, you may notice that you can't click the "Broadcast Transaction" button to send a transaction, or that you're not seeing the latest transaction in a wallet. If the slider at the very bottom right corner in Sparrow is gray, you have lost your connection. This can happen sometimes, especially after restarting or switching wifi networks.

To fix this, click on the slider to reconnect, or click **File > Preferences > Server**, to edit and test your connection.

Some warnings

Fake copies of the Sparrow site exist, at addresses that look almost right. The only real site is https://sparrowwallet.com, check the address carefully before you download.

Always be careful of any bitcoin-related software that you install. Check multiple sources to make sure you're downloading from the right website.

Extra Credit: verify the software

When using open source software—especially bitcoin software—the extra step of verifying the software is recommended. Verification is a step that confirms that the software is actually what it's supposed to be. It validates that there's no extra code snuck in, that could somehow compromise your bitcoin.

Verifying, and knowing for yourself, is one of the core principles of Bitcoin. It's embodied in the saying popular with bitcoiners: "Don't trust, verify". And it's also easier, with Bitcoin. All the core software is open source, and you can review it.

Don't trust, verify

To verify the Sparrow code, go to this page: https://sparrowwallet.com/download/. Scroll down to the "Verifying the

Release" section, and follow the steps there. This will ensure that the download wasn't corrupted with malware.

Exercise 2: Create Alice wallet in Sparrow

In this exercise, you'll create your first wallet. Wallets are the foundation of working with bitcoin, and most of the exercises in this book involve wallets. The name Alice will be used for this wallet. You can think of the wallet as belonging to Alice. Later on, you'll create more wallets, belonging to different characters.

1. Open Sparrow, and click on **File > New Wallet**. For the wallet name, type "Alice", and click **Create Wallet**. (Ignore the "Has existing transactions" checkbox now, and in the future too.)

2. Next, in the Settings window, leave everything at the defaults (policy type Single Signature HD, Script Type of Native Segwit). Below in the Keystores area of the Settings window, choose **New or imported software wallet.**

3. In the window that comes up, look for the button on the top right that says Use 24 words and **click the arrow to the right**. Choose **Use 12 words instead**.

4. A screen will pop up with 12 blank spaces for your words. At the bottom, click **Generate New** to have Sparrow auto-generate them. (Ignore the "Use passphrase?" checkbox.)
   - Sparrow will now generate a list of random words for your seed phrase.
   - They're based on a special list of 2048 unique words, called the BIP39 list. The words were chosen because they're common, easy to spell, and the first 4 letters are unique for each word.

5. **Write down the words** on a sheet of paper. Make sure to number them correctly, because the order is very important. Label the words "Alice Seed phrase".

6. Once you've written down the words, click on **Confirm Backup**. On the next screen, confirm that you've written them down. Then click on **Re-enter Words**.

7. Re-enter the 12 words, then click **Create Keystore.** Then click **Import Keystore** in the top right.
8. You're back at the main screen, the Settings window. You need to apply all the changes you've made. Click **Apply**, on the bottom right. In the Wallet Password screen that comes up next, click **No Password**.

Congratulations! You've created your first wallet.

Learn more: seed phrases and private keys

In this exercise, we asked Sparrow to generate the Mnemonic Words. These words are also commonly called the recovery phrase, backup phrase, or seed words. But the most common way to refer to these words is "seed phrase". That's what I'll use in this book.

This seed phrase represents a very large number, that's more random and impossible to guess than we can comprehend. The seed phrase is just an easy way for humans to remember and write down that number, using a specific set of common words. This list is called the BIP39 word list.

For instance, here's a sample 12 word seed phrase:

1. labor
2. stable
3. narrow
4. high
5. check
6. amused
7. young
8. rotate
9. gauge

10. fat
11. surface
12. cradle

It translates into this very large hexadecimal number:

775638ce67a669ae9fcb7e5618782bdaafe93c233ebc09469144f475b2c74b
f55f4752b51e1abb17460877c4cf9b2ae283f2e48831dc244f8d1ff5f184c1b
33f

You can see why the seed phrase is easier to write down! This number is usually called the private key. Sometimes, in more technical discussions, it's called the Master Private Key or Extended Private Key. But in this book, I'll use the term private key. We'll talk more later about how important it is to keep the seed phrase (and thus the private key) private and secure.

There are also methods for generating your own random words for a seed phrase with dice or coin tosses, without having Sparrow do it for you. I won't go into them in this book.

Learn more: wallets

Is the word "wallet" the best word to use, for what you're creating here? It's been used a long time, and it's the best word we have. But it can be misleading. It suggests that there is bitcoin actually stored in the wallet, but that's not true.

Instead of thinking of the wallet as containing bitcoin, it's better to think of the wallet as containing a key. The key that it contains is the private key, encoded from the seed phrase. The private key can unlock certain, specific chunks of bitcoin on the blockchain—any bitcoin that's associated with addresses that belong to that private key. One private key can contain many addresses.

As you work through the rest of the book, you will create these separate wallets, each with its own unique seed phrase (private key). These wallets will be named:

- **Alice**: The wallet you just created in Sparrow (Exercise 2)
- **Bob**: A second wallet that you'll create in Sparrow (in Exercise 6)
- **Carol**: A wallet that you'll set up in Blue Wallet, a popular bitcoin wallet application (in Exercise 19)
- **Dan**: A wallet you create as a bonus final exercise, in Blockstream, which is another multi-platform bitcoin wallet (in Exercise 27)

Although you will create a few other wallets, they will all be derived from one of these four.

Though we're naming wallets after people (like Alice and Bob), this is just to make it easier to understand. But one person *can* have multiple wallets, for different purposes. For instance, Alice may have a Cold Storage wallet, and a Spending wallet, just like you might have a savings account and a checking account at a bank.

Using these different wallets, in multiple bitcoin wallet applications, you'll gain hands on experience with many user interfaces. This approach is an excellent way to master the fundamentals of Bitcoin, and to learn the skills needed to safely hold, send, and receive bitcoin.

Exercise 3: Buy Bitcoin

In this step, you'll actually purchase bitcoin, using whichever source you prefer from the options given below. In the exercise after this one, you'll move some of that bitcoin to the wallet you created in Exercise 2.

How much will you buy? Choose an amount that you're comfortable with, probably less than 50 to 100 USD, or the equivalent in other currencies.

This should be an amount small enough that you're not worried about losing it, but large enough to be able to do all the exercises. You'll pay transaction fees to move the bitcoin around to different wallets, but depending on the current transaction fees, most of the bitcoin will left at the end. You'll learn more about transaction fees as you go through the exercises.

A reminder—when you're buying bitcoin in this step, you're *not* buying it on an exchange traded fund (ETF), because then you wouldn't be holding and managing your own bitcoin. Instead of ETFs, you're buying bitcoin that you can receive into your own wallet, in self custody.

Since there's so many different sources to buy bitcoin from, I can't walk you through the process of setting up an account and buying bitcoin, because it will be different everywhere. But I'll give you some general thoughts about the best ways and sources to buy from.

Also, a note about keeping your bitcoin safe. At this point, you just need to take very basic security precautions. This is because:

- The amounts that you're dealing with are very small.
- The wallets you're working with are temporary. Once you've finished the exercises, you'll send the bitcoin to another wallet.

Where should you buy bitcoin? KYC or P2P

There are two main ways of buying bitcoin, KYC ("Know Your Customer") and P2P (Peer To Peer).

KYC is what most people use, in countries where exchanges are available. It means using a centralized exchange, which follows government "Know Your Customer" laws. On a KYC exchange, you need to open an account, linked to your government ID, to purchase bitcoin. You will need to go through an identity verification process. This usually includes submitting photos of government-issued ID, as well as facial scans. It may take a few days.

P2P means you're not going through a regular exchange. Instead, you're buying from a peer—someone who owns bitcoin and wants to sell it.

If you're lucky enough to have a friend or family member who's willing to sell you a small amount of bitcoin, then the transaction can be very simple. You hand the friend or family member some cash, and give them a bitcoin address from your wallet. Then they send you the bitcoin (minus the transaction fee).

But often, P2P trades will be done online, via one of the secure, private services mentioned below.

One of the main benefits of buying P2P is increased privacy. If you're buying peer to peer, the only other person that knows about the purchase is the seller. However, if you're buying from a KYC exchange, your personal information is available to both the exchange, and the government. And considering how often companies have been hacked and their customer database stolen—it's not just the government who could get your data. Criminal gangs could get it as well.

The problem for people just starting to buy bitcoin is that for some of these P2P services, you need to already own at least a small amount of bitcoin, for the escrow/bond service.

KYC Exchanges

If you've decided that for now, you'll use a KYC exchange, you have many options.

It's important to purchase from a bitcoin-only exchange. An exchange that is bitcoin-only will have fewer points of failure. And more importantly,

they won't try to sell you other, inferior cryptocurrencies, that they make better commissions on. Companies that sell anything other than bitcoin—exchanges such as Coinbase, Kraken, Robinhood, Binance—are not recommended. (However, if you already own bitcoin through one of these sites, feel free to use it for these exercises.)

There's a saying among bitcoiners that expresses a core belief—that Bitcoin stands alone, and is fundamentally superior to other cryptocurrencies.

Bitcoin, not crypto.

When you're picking a KYC exchange, make sure that they will actually allow you to withdraw your bitcoin, to your own wallet. The below list is not an exhaustive list, and this information can change quickly, so do your own research.

Here's some KYC exchanges that are Bitcoin-only.

Strike (Many countries)	https://strike.me/
Swan (US)	https://www.swanbitcoin.com/
Unchained Capital (US)	https://unchained.com/
River (US)	https://river.com/
Cashapp (US, UK)	https://cash.app
Relai (Europe, Swiss-based)	https://relai.app/
Bull Bitcoin (Canada, Europe)	https://www.bullbitcoin.com/

P2P exchanges

In general, using a P2P exchange can be a little more challenging. Also, even more so than with KYC exchanges, you'll need to stay informed because the P2P markets can change quickly. But on the plus side, you get the best possible privacy, and that's worth a lot.

Below are some of the more common P2P exchanges. For more options, take a look at this site: https://kycnot.me/.

Robosats	https://learn.robosats.org/
Bisq	https://bisq.network/
Peach	https://peachbitcoin.com/
Hodl Hodl	https://hodlhodl.com/
Vexl	https://vexl.it/

If you don't own any bitcoin yet, start with Hodl Hodl, Vexl, or Bisq's "Bisq Easy" mode—none of these require an upfront bitcoin deposit.

Robosats requires a Bitcoin Lightning wallet in order to use it (see the Lightning Network chapter towards the end of this book for more information), but it’s one of the most popular and easiest P2P exchanges.

One more note if you use both KYC and non-KYC methods: keep them in separate wallets. Combining them links the private coins to your identity, undoing the privacy you paid for.

In the next exercise, you will need to have already completed the purchase of bitcoin. It needs to be ready to send, from the exchange to your own receive address.

Exercise 4: Receive bitcoin into your Alice wallet

In this exercise, you'll actually receive bitcoin into your wallet. The procedure will be a little different on each exchange. Some exchanges may even require you to get approval for the receive address.

But basically, it will involve steps similar to this:

- Open up the website or app for your exchange (where you bought the bitcoin), and navigate to where you can send bitcoin out of the exchange.
- Enter a bitcoin address. (This will be a receive address that you get from the Alice wallet).
- Decide how much you want to send. It's easier to think of bitcoin amounts in terms of sats, because 1 bitcoin is now very expensive. (Sats is short for Satoshis. One whole bitcoin equals 100 million sats.)
- Enter the amount of sats you want to send to the Alice receive address.
- Decide on the amount of fees you're willing to pay. Some exchanges may pay the transaction fees for you.
- Hit the send button, and wait for the bitcoin to arrive in your wallet.

Example: Using Strike to receive bitcoin

These are what the steps look like when sending bitcoin from Strike, the KYC exchange that I mentioned above. Remember, the process in the exchange that you use will be different. Using Strike (which is a mobile app on your phone), it's easiest to use QR codes to get the bitcoin receive address, instead of copying and pasting the address.

1. In Sparrow on your computer, open up the Alice wallet file. Click **Receive** in the blue bar on the left. Your wallet has many, many receive addresses, and Sparrow will show you the first available

address. Notice that some characters are black, and some are gray—this is to make it easier to read.

2. Label the receive address. I wrote “Receive from Strike” in the label. When using the defaults in Sparrow, all bitcoin addresses start with bc1. The QR code for the address, which I’ll use in the next step, is to the right of the address.
   Don’t skip the label! Some of the following exercises depend on having labels.

3. In the Strike app on my phone, I tap the Bitcoin icon at the bottom left. I scroll to the Send screen, and tap Bitcoin wallet.
   Then I go back to Sparrow on my computer, where the Receive window is still open. I use Strike on my phone to scan the Sparrow QR code for the receive address.

4. In Strike, I enter the amount of sats that I want to send (it’s about half of what I purchased, make sure it’s a small amount that you won’t worry about losing).

5. Next is the fee. I could either pay a larger fee, to have the transaction go through in the next 10 minutes, a medium fee to send it in the next hour, or zero, to have it go through in the next 24 hours.
   I chose to pay the higher fee, and have it go through within about 10 minutes. Other exchanges will have different options for fees.

6. On the next screen I review the details (amount, receive address), before tapping to confirm the transaction.

If the exchange you’re using is a desktop application, and not a mobile app, you’ll need to copy and paste the bitcoin address, instead of using a QR code.

Monitoring the receive into Alice

You will now receive the bitcoin into your Alice wallet, in Sparrow. No matter where the bitcoin originally came from, here’s what you should see as the transaction goes through.

If you've chosen to pay a higher fee for a quicker transaction, it may all happen within about 10 minutes. Otherwise, it will take longer, anywhere from about 10 minutes to a day or more.

1. The first step is that you get a pop-up notice in the top right corner, in Sparrow. It'll have a message entitled "New mempool transaction", and the amount of the transaction. These Sparrow notifications disappear after a few seconds.
   That means your transaction is in the mempool. (See the below section "Learn more: Mempool and Blockchain" for more info.)

2. Once you've gotten the pop-up notice in your Alice wallet, click on the **Transactions** in the blue bar on the left. You should have one transaction in there, from the transaction you just made. The transaction will show up in light gray at first.

3. You'll receive another pop-up notification in Sparrow when the first confirmation occurs, which is usually in about 10 minutes. Six confirmations is usually considered final, and then the transaction in Sparrow will switch from light gray to black.

4. Notice that in the Transactions window, there's a US dollar amount in there. For the dollar amount, the current bitcoin price is used. (To set up a different default currency, go to File > Settings > Currency.)

Congratulations! You now truly own some bitcoin, it's on your own personal wallet, and you have the private key.

Troubleshooting your connection in Sparrow

This was also mentioned in Exercise 1, but here's a reminder, because it sometimes happens. You may notice that a transaction doesn't show up when it should. If this happens, check the slider at the very bottom right corner in Sparrow. If it's gray, you have lost your connection.

To fix this, click on the slider to reconnect.

Learn more: Mempool and blockchain

The mempool is a holding area for bitcoin transactions that have been submitted, but not yet added to a block. It's like bitcoin's waiting room—an area where transactions sit before being included in a block. When you send bitcoin, your transaction joins others in the mempool, waiting for bitcoin miners to pick them up.

After a miner picks them up and confirms them in a new block, the block gets added to the bitcoin blockchain. This means that the transaction has one confirmation. When another block gets added to the blockchain, your transaction will have two confirmations. Once it has six confirmations, most people consider that "final settlement"—in other words, it's almost impossible to reverse.

What is the blockchain? It's like a giant public notebook, or ledger, of all the transactions that have ever occurred, in separate blocks. By looking at the blockchain, you can see exactly what the transactions were, the amounts of the transactions, and the sending and receiving address.

You pay a fee, called the transaction fee, for having your transaction included in the next block, and added to the blockchain. This can be higher or lower, depending on how much competition there is for transaction space in the bitcoin blockchain. Transactions that include higher fees get chosen first by the miners, and go into the very next block. Lower-fee transactions wait longer. We'll discuss fees in more detail later.

Learn more: bitcoin mining

Just now, in the section on Mempool and blockchain, the term bitcoin miners came up. What is, actually, the process of bitcoin mining?

Basically, bitcoin mining happens with a decentralized network of special computers ("miners"), all around the world. All of these miners are competing to solve a mathematical problem, and the average time it takes for one of them to find the answer is about 10 minutes. Whichever computer finds it first gets to "mine" the next block of transactions, which means linking the new block to the previous one in the blockchain.

Bitcoin mining takes special, expensive computers, and lots of electricity. The reason that the miners do this work is that they earn bitcoin in two different ways, each time they mine a block.

- There's a reward in bitcoin, for the computer that mines that block. This reward is substantial. Right now, each mined block earns 3.125 bitcoin.
- Also, the successful miner gets to keep the transaction fees associated with the block.

The reward in bitcoin for the successful miner is straightforward, it's just a set amount.

The transaction fees are more complex. Every single transaction needs to pay a fee, to pay for the work of putting it in the block. And transaction fees depend on how busy the network is. If many people are trying to make transactions, fees go up because there's more competition for a scarce resource—space on the bitcoin blockchain.

It's similar to when a city is hosting the Olympics. Hotel rooms will get much more expensive because there's only a set amount of them. Similarly, you will have to pay more in transaction fees when the bitcoin network is congested.

Luckily, transaction fees have recently been very low, so the transactions you'll be making in these exercises will be inexpensive.

Exercise 5: Recover your Alice wallet

Being able to recover your wallet is an important step in Bitcoin security. If something unexpected happens, you need to be able to gain access to your bitcoin again with just your seed phrase.

So, practicing recovery is a must, when learning to use bitcoin.

1. In Sparrow, close the original Alice wallet. Click on **File > New Wallet**. Name the wallet "Alice Recovery" and click on **Create Wallet**.
   Note that we're creating a new wallet file in Sparrow here, but it will be derived from the original Alice wallet, and will have the same seed phrase (private key).

2. You're now in the Settings window. Leave the settings as they are (Single Signature HD, Native Segwit). At the bottom in the Keystores section, click **New or Imported Software Wallet.** In the next window, look for the button on the top right that says Use 24 words and **click the arrow to the right.** Choose **Use 12 words** instead.

3. Enter in the 12 words you wrote down in the exercise "Create a wallet in Sparrow—Alice". Don't create a passphrase. Click the **Create Keystore** button.

4. Leave the derivation path at the default of m/84'/0'/0', and click on **Import Keystore**.

5. Now at the bottom right corner of your screen, click the **Apply** button. On the next screen, click **No password** on the "Wallet Password" screen.

6. You have now recovered your Alice wallet. Click **Transactions** in the blue bar on the left, to switch to that window. You should be able to see the transaction you made earlier.

7. Also check the addresses, between the original and the recovered wallet. To do this, open the original Alice wallet, and click on Addresses in the blue bar on the left. Do the same in the Alice Recovery wallet.

8. Cross check the first few Receive addresses between the two wallets. Make sure they're the same. If the addresses are the same, and you see the previous transaction, you've restored the wallet correctly. Congratulations!

Learn more: wallet recovery

It's a good idea to practice recovering a wallet occasionally. If you lose your computer, or the Sparrow wallet file, or lose your hardware wallet, you can still recover your wallet—but only if you kept the seed phrase safe.

But if a disaster happened *and* you didn't have your original seed phrase or a backup, then unfortunately you've lost your funds. You no longer have access to your bitcoin, and you can't recover from that.

Common problems when recovering wallets

Some of the common problems that occur when recovering wallets are:

- Missing a Passphrase
- Differences in Script Type

We'll go over both of these issues in more depth in upcoming exercises.