| * Chapter 7: How to Use Bitcoin   + 7.0 Introduction   + 7.1 Acquiring and exchanging bitcoin     - 7.1.1 P2P: physical     - 7.1.2 P2P exchanges: online     - 7.1.3 Centralized exchanges   + 7.2 An introduction to Bitcoin wallets     - 7.2.1 Self-custodial vs Custodial wallets     - 7.2.2 Different types of Bitcoin wallets     - 7.3.3 Open Source vs Closed Source     - **Activity** - Class evaluation of Bitcoin wallets   + 7.3 Setting up a mobile Bitcoin wallet     - **Activity** - setting up/recovering a Bitcoin Wallet   + 7.4 Receiving and Sending transactions     - **Activity** - Bitcoin Transactions in Action   + 7.5 Saving in bitcoin   + 7.6 DYOR - Don’t Trust, Verify |
| --- |

# 

# Chapter 7: How to Use Bitcoin

## 7.0 Introduction

“Why would anyone trust nerd money vs central bank money? Nerds brought you the internet.

Banks brought you the great depression.”

Andreas M. Antonopoulos

Now that we have a better understanding of what Bitcoin is and its purpose, it's time to learn how to use it practically. In this chapter, we'll guide you step-by-step through the process of acquiring Bitcoin, explore the various types of wallets available, help you set up your own Bitcoin wallet, and even practice sending and tracking a Bitcoin transaction on the network. It's time to turn your understanding into action!

## 7.1 Acquiring and exchanging bitcoin

There are many ways to acquire bitcoin. For example you can:

1. Get paid in bitcoin in exchange for your work, and pay for other people’s products and services with bitcoin. (more on that in Chapter 8)
2. Mine bitcoin (more on that in Chapter 9)
3. Exchange your fiat currency for bitcoin, or exchange your bitcoin for fiat currency in person.
4. Exchange your fiat currency for bitcoin, or exchange your bitcoin for fiat currency online.

[Image from Chapter 7 Images Folder]



Below, we’ll explore exchanging fiat currency for bitcoin, and vice versa, both through in-person transactions and online methods, as they are the most common options.

**7.1.1 Peer to peer in person**

Engaging in peer-to-peer (P2P) transactions for acquiring and selling bitcoin involves directly exchanging your fiat currency (or any other good or service) for bitcoin with another individual, eliminating the need for a bank or other party to be involved in the transaction.

Both parties mutually determine the exchange amount and rate. The buyer provides the cash, the seller transfers the bitcoin, and the transaction concludes.

While it’s easier to do P2P exchanges physically by meeting with the other individual directly in the real world, you can also do so from virtually anywhere, thanks to the internet. Additionally, exchanging bitcoin for fiat currency follows a similar process in reverse.

[Image from Chapter 7 Images Folder]



**7.1.2 Peer to peer online**

Enter P2P platforms, where Bitcoin buyers and sellers meet in cyber space to conduct transactions without any intermediaries, directly on the internet.

With such platforms, you don’t have to trust anyone with your information or your money, you can meet other peers and trade with them directly.

[Image from Chapter 7 Images Folder]



On most P2P platforms, peers have to escrow some of the funds to ensure they will comply with their part of the deal. Escrow means putting the money in a safe place that the platform controls until both parties do what they promised. It's like a trusted friend holding onto your stuff until everyone keeps their word.

**7.1.3 Centralized exchanges**

Using centralized exchanges may be the easiest way to acquire and sell bitcoin, but it also involves significant trade-offs. Centralized exchanges are companies that allow clients to buy and sell bitcoin directly through them. However, this convenience comes at a cost.

[Image from Chapter 7 Images Folder]



Centralized Exchanges and their tradeoffs

It’s important to note that when buying bitcoin through a centralized exchange, you are often required to provide personal information and verify your identity. This creates a risk of identity theft and exposes your personal information to potential threats. Additionally, centralized exchanges hold your bitcoin for you, which means you are not in control of your money until you withdraw it from them.

To add to the concerns, centralized exchanges can misappropriate users’ funds or lend more bitcoin than they have in reserves until they collapse. Yes, just like banks! However, in the Bitcoin world, there is no central bank to bail out fraudulent banks by printing more currency, because you can't print more bitcoin!

## 7.2 An introduction to Bitcoin wallets

Unlike physical money, bitcoins are not actually present in a Bitcoin wallet. They live on the distributed ledger that the Bitcoin network constantly verifies and secures. So how can you own bitcoin?

[Image from Chapter 7 Images Folder]



You have ownership of your bitcoin only when you own the private keys that allow you to sign transactions and transfer ownership of your bitcoin from you to someone else. This is the act of sending bitcoin.

With that in mind, let’s take a look at 2 concepts we describe when using the term “wallet”:

1) A master private key (which is like a password) from which you can generate public keys which you can share with others to receive and send bitcoins.

2) The mobile or desktop interface from which you can interact with the Bitcoin network to retrieve your bitcoin balance, send and receive transactions, and broadcast them to the network. Different types of wallets, along with their benefits and tradeoffs, will be described in the next section.

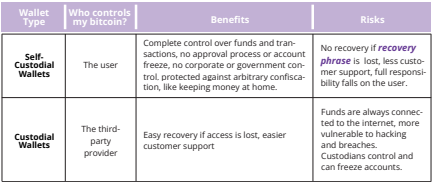
**7.2.1 Self-custodial vs Custodial wallets**

Before going into the details of the different types of Bitcoin wallets and their characteristics, let’s make an important distinction between self-custodial and custodial wallets.

This table includes the two main types of Bitcoin wallets, self-custodial and custodial. You can

see the benefits and risks of using each wallet type and who controls the bitcoin in each case. Self-custodial means the user holds the private keys, which means they are in true possession of their bitcoin, while with the second type, a third party holds their bitcoin.

[Image from BD 2023 page 102]



In a self-custodial wallet (also called non-custodial wallet,) you are the only one with the keys to

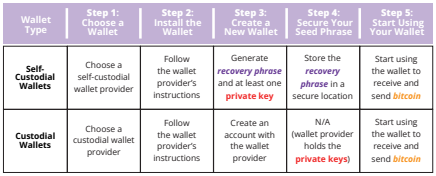
the wallet and you have full control over what goes in and out. On the other hand, in a custodial

wallet, someone else holds the key and can access and manage the contents of the wallet on your behalf.

* Self-custody is like being your own bank. Transactions are not subject to control or authority by any government or company, but it also means you bear full responsibility for keeping your bitcoin secure.
* Self-custody ensures that third parties cannot confiscate your bitcoin without your consent.
* Self-custody gives peace of mind in times of uncertainty, knowing your bitcoin is secure.

It’s important to choose the right type of wallet for each individual’s needs. Sometimes people find it hard to distinguish whether they are installing a self-custodial or a custodial wallet. This table shows the differences in installation process.

[Image from BD 2023 page 104]



[Image from BD 2023 page 106]



“Not your keys, not your coins” is a popular saying among Bitcoin holders. It refers to the idea that if you don’t have direct control over the private keys associated with your Bitcoin wallet, you don’t have true ownership of the coins.

Whoever accesses your private keys will gain ownership of your bitcoin. This is why it is of the utmost importance to protect them by keeping them away from prying eyes! We’ll see a few ways you can do that later in the book.

For what follows, we’ll be talking about self-custodial wallets only, where the user owns their own keys and has complete control over their bitcoin.

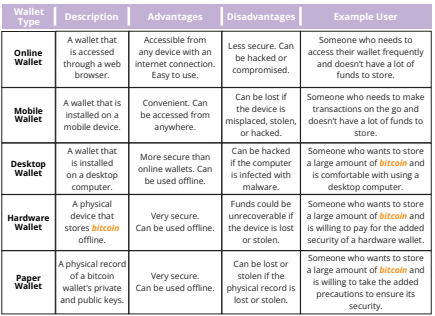
Don’t worry if it gets complicated or you don’t understand everything. This is a journey and you will understand more as you start using Bitcoin more!

**7.2.2 Different types of Bitcoin wallets**

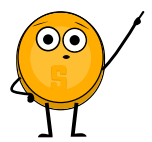
Depending on where your private key is created and stored, we commonly use different names to describe Bitcoin wallets.

If the keys are stored on your smartphone, we can call it a “mobile wallet”. If they’re stored securely on a dedicated device, we’ll call it a “hardware wallet”. If the key is only stored on paper, then it can be called a “paper wallet”.

Here’s a table presenting the different names we give to Bitcoin wallets, depending on the structure they have:

[Image from BD 2023 page 104]  


Because the keys can be moved from one device to another, the “status” of your Bitcoin wallet is not definitive. For example, if I generate the keys of my Bitcoin wallet on a computer and later upload them to my phone, the “desktop wallet” then becomes a “mobile wallet”.

[Image from BD 2023 page 103]

When it comes to storing your bitcoin, it’s not just about who has control over it - there are many other risks to consider as well. That’s why it’s important to find a storage solution that is both secure and convenient.

When you analyze the trade-offs of the various types of wallets, you will learn there is no ideal wallet that satisfies all needs.

When choosing a Bitcoin wallet, there are several things you should consider:

* Security: Make sure the wallet has strong security measures in place, such as two-factor authentication and secure password policies.
* Privacy: Consider whether the wallet allows you to remain anonymous, or if it requires personal information to set up an account.
* Ease of Use: Choose a wallet that is easy to use and navigate, especially if you are new to Bitcoin.
* Compatibility: Make sure the wallet is compatible with your device and operating system.
* Fees: Compare the fees charged by different wallets to make sure you are getting the best deal.
* Reputation: Research the reputation of the wallet and its team to make sure it is trustworthy.
* Control: Some wallets give you more control over your private keys, which can be a security advantage.

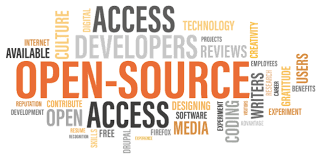
Consider whether you want a wallet that gives you full control, or one that is more user friendly but may have less control.

**7.2.3 Open Source vs Closed Source**

Another important factor to keep in mind when choosing a Bitcoin wallet is knowing if the application or software is open-source or not.

Open-source code is very important, because it allows the community to review the code and continue developing the project if the team were to stop working on it.

[Image from Chapter 7 Images Folder]



Just as Bitcoin’s code is completely open for everyone to review, use and modify, so should be the code of the wallet you use to store your bitcoin.

**Activity - Class discussion and evaluation of Bitcoin wallets on bitcoin.org**

Go to the following website: <https://bitcoin.org/en/choose-your-wallet> and use your new knowledge of Bitcoin wallets to select the best one based on the criteria we discussed today. 

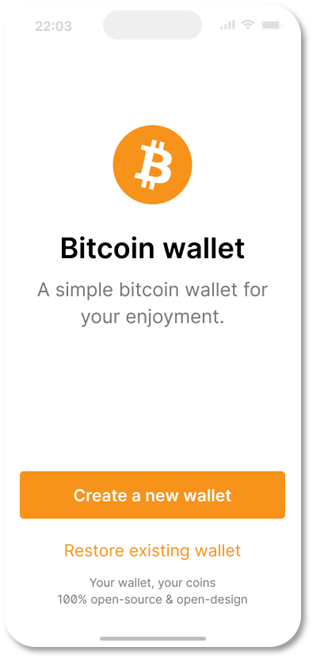
## 7.3 Setting up a mobile Bitcoin wallet

Now that we have a better understanding of Bitcoin wallets and the differences between them, we’ll see how to use one in practice. For this example, we’ll create a mobile wallet directly on our smartphone.

**Activity - setting up/recovering a Bitcoin wallet**

If students do not have cell phones, the teacher will provide one to each student to borrow.   
  
There are two options for this activity:

| **Class Exercise. Option 1. Download a new wallet.** |
| --- |

[Image from Chapter 7 Images Folder]

**How to create and use a Bitcoin wallet.**

1. Search for the app in the App Store (iOS) or Google Play Store (Android).

2. Open the app and type in your 12- or 24-word recovery phrase (sometimes called a seed phrase). **Be sure to write it down and keep this in a safe place!** This recovery phrase allows you to recover full access to your funds if needed.   
  
**Remember that if you lose or forget this sequence of words, you will not be able to access your bitcoin if you lose access to your wallet.**

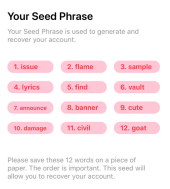
3. **You must then confirm** that you have actually saved your recovery or **seed phrase.** To do this, you must **enter**, in the same order, the **words** of your seed phrase.

4. As an additional measure of security, some wallets allow you to **choose a secure password**. Your **private key** and first **bitcoin address** are automatically created for you by your wallet.

| “ORANGE IDEA BOX”  Think of your public address as your email address – you want to share this with others so they can send you bitcoin, or in the case of an email address, an email.   Think of your private address as the password to your email – you wouldn’t want to share this with anyone as it would give them access to your email. |
| --- |

5. Use your “**receive**” address to receive bitcoin. **Transfer bitcoin to your wallet.** With a self-custodial wallet, you cannot always buy **bitcoin** directly with fiat, so you might need to purchase and transfer it from an exchange first.

[Image from BD 2023 page 104]



| Class Exercise. Option 2. Restore Wallet (Time Limited). |
| --- |

**Download a bitcoin wallet** and add some satoshis for each student.

Give each student a sheet with a seed phrase to retrieve a wallet.

Guide students step by step:

[Image from Chapter 7 Images Folder]



1. When you first start your wallet, you will see three methods of wallet creation, tap **[Import an existing wallet]** You will see an introduction screen, tap **[Restore with recovery phrase]**

2. Enter your 12/18/24-word recovery phrase one by one, in the correct order.

3. Touch **[Restore]** when finished.

4. You will see an “Import Successful” mode when your wallet has been successfully imported.

## 

## 7.4 Receiving and Sending transactions

A Bitcoin transaction is a transfer of ownership of existing bitcoin to a new owner. But instead of transferring actual coins, all the nodes in the network update their local copy of the public ledger to reflect the change in ownership.

When sending a Bitcoin transaction, the sender signs a message that only they can sign with their private key, signaling to the network that the ownership of the bitcoin changes to the recipient’s address.

The bitcoin will now be tied to an address that only the new owner can send from, giving them ownership of the bitcoin.

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

**Source the first part of section 7.4 from section 5.3 on page 91-92 up until the “now with a bit of detail” part.**

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

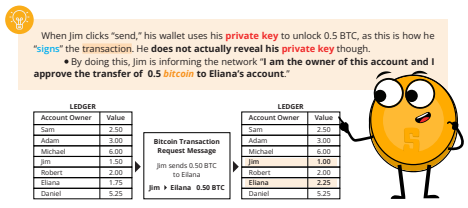
New Bitcoin transactions are initiated from wallets around the world, but there is no central payment processor. Instead, miners around the world compete to record transactions in the ledger.

Let’s say Jim owes Eliana 0.5 BTC and is ready to pay her back. Both have digital wallets.

1. Eliana shares her address with Jim.

2. Jim uses his wallet software to create the transaction, which includes Eliana’s address, the amount to be transferred (0.5 BTC), and a fee for the miner.

[Image from BD 2023 page 91]



3. After signing the transaction, it is broadcast to the network where it is verified by nodes.. Nodes check the transaction for validity and ensure that Jim has enough funds. If he does not, they reject the transaction immediately.

4. Once the transaction is verified, it is added to the blockchain by miners, and the funds are transferred to Eliana’s address.

5. Eliana can then use her private key to access the transferred funds in her wallet.

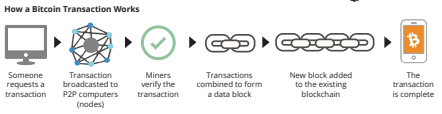
It’s important to note that once the transaction is complete, it cannot be reversed.

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

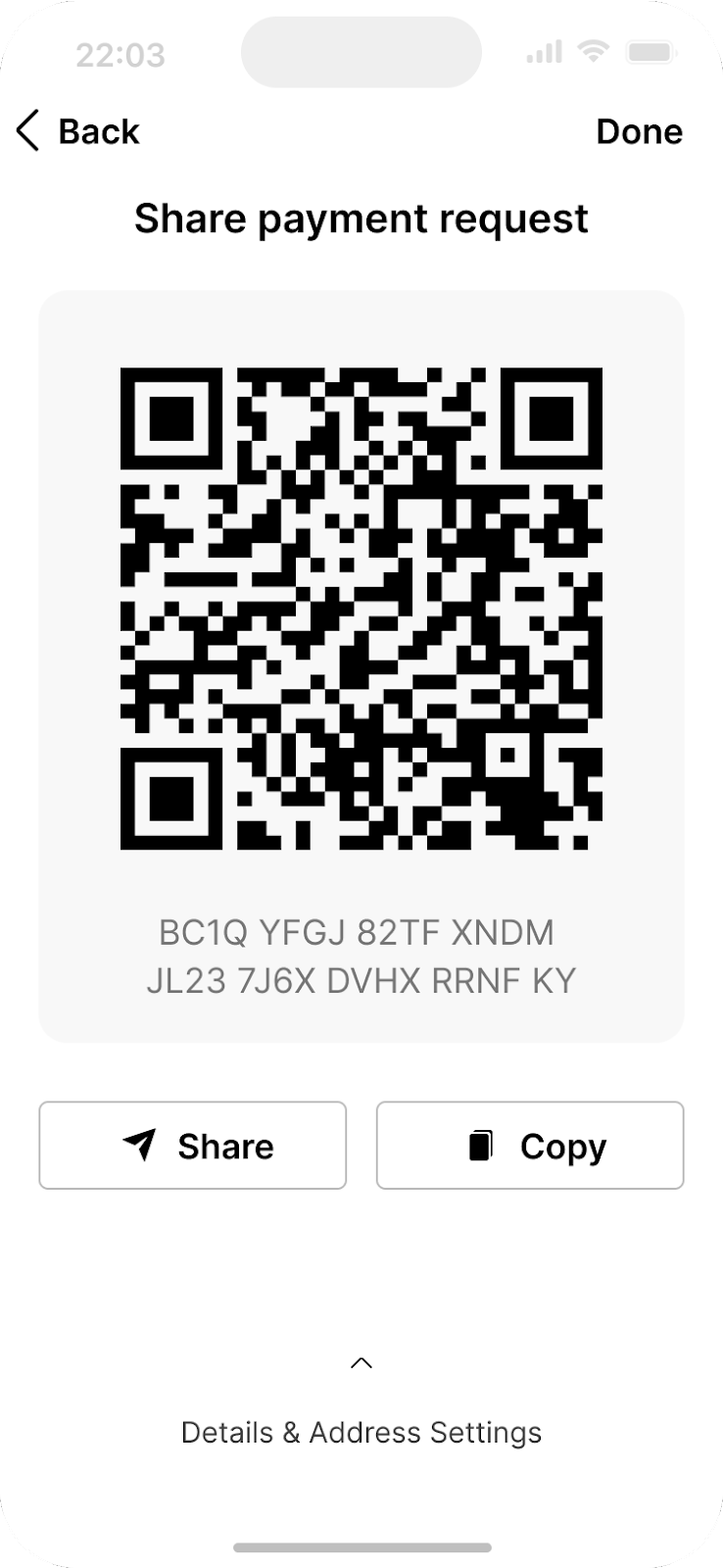
**Image below titled How a Bitcoin Transaction works sourced from page 95**

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

[Image from BD 2023 page 95]



**Receiving Bitcoin transactions:**

[Image from Chapter 7 Images Folder]

To receive bitcoin, you will need to provide the sender with your bitcoin wallet address. This is a unique string of letters and numbers that represents your wallet and is used to identify it on the Bitcoin Network. You can find your wallet address by logging into your Bitcoin wallet and looking for an option to “Receive” or “Deposit” bitcoin.

You can then share your bitcoin address with the sender in one of several ways:

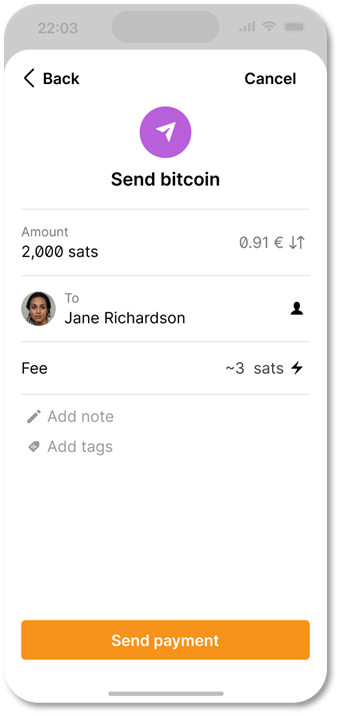
1. Copy and paste the address: You can copy the address by highlighting it and pressing “Copy” on your keyboard, then paste it into an email or message to the sender.
2. Share a link to your Bitcoin wallet: Some Bitcoin wallets allow you to create a link to your wallet that you can share with the sender. They can then click on the link to access your wallet and send the bitcoin.
3. Share a QR code: If the sender has a smartphone with a Bitcoin wallet app, they can scan the QR code to get your bitcoin address.

Once the sender has your bitcoin address, they can send you the bitcoin by entering your address and the amount they want to send you and initiate the transaction. The bitcoin will then be sent to your wallet and will be visible once the transaction is confirmed on the Bitcoin Network. This usually takes a few minutes.

Next, we will take a look at sending bitcoin transactions.

**Sending Bitcoin Transactions:**

[Image from Chapter 7 Images Folder]

To send bitcoin, you will need a few things: a Bitcoin wallet, the recipient’s bitcoin address, and the amount of bitcoin you want to send.

1. Open your Bitcoin wallet. A SMS code will be sent to your phone number, and you will need to enter it in the dialog box. Alternatively, if you have enabled Google 2FA, you will need to enter the six-digit code from the Google Authenticator app

2. Navigate to the “Send” or “Withdraw” feature and copy the recipient’s address.

3. Enter the recipient’s bitcoin address by pasting it in the “To” field.

4. Enter the amount of bitcoin you want to send in the “Amount” field.

5. Double-check the recipient’s address and the amount to be sent.

6. Before clicking Confirm and Send, **we recommend that you double-check the transaction details one more time to ensure that you are sending the correct amount of bitcoin to the correct wallet address.**

7. Confirm the transaction and wait for the network to confirm the transaction.

Now you know how to evaluate, select, and set up a self-custodial Bitcoin wallet. Sending bitcoin from one wallet to another on the Bitcoin network is called sending an “on-chain” transaction. This is because the transaction occurs on the main Bitcoin network blockchain. On-chain transactions are the safest way to transact with bitcoin; however, transactions are more expensive and slower than other options we will discuss in Chapter 8.

**Activity** - **Bitcoin Transactions in Action**

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

**Source the Activity and images from** **Bitcoin Transactions in Action from** Section 5.3.1 page 95)

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------

Objective: To understand the underlying concepts and mechanics of a peer-to-peer Bitcoin transaction.

Before we get started, here’s a quick reminder on the key players in a Bitcoin Transaction:

1. Senders and Receivers are the parties who wish to transact with each other.
2. Nodes validate transactions and store a complete copy of the blockchain. \*Light nodes let people validate transactions while using less storage and fewer computational resources.
3. Miners are responsible for adding new transactions to the blockchain.

Understand your role. You have been assigned one of the following roles: **sender, receiver, node, or miner.**

* Senders will be responsible for creating and broadcasting transactions.
* Receivers will be responsible for receiving and verifying transactions.
* Nodes will be responsible for validating the transactions by checking that the transaction is valid.
* Miners will be responsible for adding the transactions to the blockchain.

1. **As a sender:** Create a transaction.

* To create a transaction, follow these steps: Take a transaction note and write the number of coins you want to send and the name or initials of the receiver. Sign the note with your name or initials, simulating a private key. Pass the transaction note and the corresponding number of coins to the receiver.

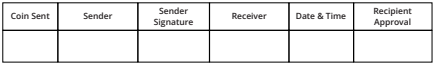
**Both nodes and receivers have to verify transactions:**

2. **As a receiver:** You are responsible for verifying the transactions.

Follow these steps:

* Check the transaction note to ensure that the correct number of coins and the receiver’s name or initials are written.
* Count the coins received and compare them to the number of coins written on the note.
* If the coins match, check the approval box. If the coins do not match or you have doubts, reject the transaction

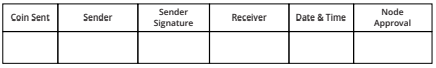
[Image from BD 2023 page 96-97]



3. **As a node:** Verify and validate transactions. You are responsible for checking that the transaction is valid.

* Verify that the sender’s address is valid and that the receiver’s address is valid.
* Check that the sender has enough funds to complete the transaction and that the transaction does not double-spend any coins.

[Image from BD 2023 page 96-97]



4. **As a miner**: add transactions to the blockchain. You are responsible for adding the transactions to the blockchain.

Follow these steps:

* Check the transactions that have been approved by the receivers and validated by the nodes.
* Roll the dice and compare the numbers with the other miner. The miner with the smaller number will add the transaction to the blockchain.
* For your time, energy, and effort, you will earn a point. At the end of the activity, the miner with the most points wins.

\*\*Once a transaction is added to the blockchain, it cannot be changed or reversed.

5. Keep track of your coin balance: Throughout the activity, keep track of your coin balance by counting the coins in your digital wallet.

[Image from BD 2023 page 96-97]



6. Discuss the concepts learned with your class.

## 7.5 Saving in bitcoin

Bitcoin is a way to safeguard your money against inflation and protect it from being controlled by anyone else, if you do it correctly. Saving in bitcoin provides a vehicle to store, accumulate and build wealth over time. As you understand by now, the type of money you choose to save is one of the most important decisions you can make. Choosing wisely allows you to build a better future for yourself and your family.

[Image from Chapter 7 Images Folder]



**Peace of Mind:** When stored properly, Bitcoin is the only form of property nobody can take away from you.

[Image from Chapter 7 Images Folder]



## 

## 7.6 Don’t Trust, Verify

Whatever you do in Bitcoin, remember this: “Don’t Trust, Verify”. There are no leaders in Bitcoin. You should never blindly follow someone’s claims. Rather, you should always question what you’re being told, and verify it for yourself. By following this mantra, you’ll protect yourself from losing your bitcoin. This goes for claims such as “the next Bitcoin” just as it does for “investment opportunities” or promises of “quick and easy profits”.

In summary, Chapter 7 has given you the important skills to use Bitcoin in your everyday life. You have learned how to get and exchange bitcoin in different ways and how to keep it safe using various wallets.

By setting up your mobile Bitcoin wallet and doing transactions with others, you now have hands-on experience to confidently use bitcoin day-to-day. Understanding Bitcoin as a way to save money and following the idea of "DYOR - Don’t Trust, Verify," you're now in control of your money.

In the upcoming chapter, we will explore the Lightning Network. We will look at how this innovative technology is changing the way people worldwide access and use money. From everyday transactions to more advanced applications, you will learn how the Lightning Network empowers individuals, communities and businesses by providing them access to financial services.

—-------------------------------- Notes only - Below not in 2024 workbook —---------------------------

* + ***Notes to designer:***
    - **Source images tagged “**[Image from Chapter 7 Images Folder]” from: <https://drive.google.com/drive/folders/1P42n5nuRnyoRb-Gc-s__d5QE093LL72_?usp=sharing>

—---------------------------- Notes only - Above not in 2024 workbook —---------------------------------