757btc Meetup

Bitcoin education based on the open-source content from My First Bitcoin
myfirstbitcoin.io

Chapter 7

757btc.org

Follow on nostr

My First Bitcoin
EL SALVADOR

Bitcoin Diploma

Financial Education for the Bitcoin Era

Acquiring and Exchanging Bitcoin

> Why would anyone trust nerd money vs. central bank money? Nerds brought you the internet. Banks brought you the Great Depression.
>
> **Andreas M. Antonopoulos**

- Get paid in bitcoin in exchange for goods/services
- Mine bitcoin (more on mining in chapter 9)
- Exchange in person
- Exchange online

Peer-to-Peer

Peer-to-peer (P2P) transactions involve directly exchanging your fiat (or goods/services) with another individual, eliminating the need for a bank or third party to be involved

P2P transactions can be done in person or online. Both parties mutually determine the exchange amount (for goods/services) or rate (for fiat)

Online P2P platforms normally require to have parties escrow some of the funds to ensure they will comply with their part of the deal

This means that the money will be put in a safe place that the platform controls until both parties do what they promised

Centralized Exchanges

Using centralized exchanges may be the easiest way to acquire/sell bitcoin, but this involves trade-offs

Centralized exchanges comply with KYC (Know Your Customer) rules which requires you to provide personal information and verify your identity with the exchange

CENTRALIZED

These exchanges can also misappropriate users' funds or lend more bitcoin than they have in reserves until they collapse (sound familiar?)

In the bitcoin world, there is no central bank to bail out fraudulent banks by printing more currency

Bitcoin Wallets

Unlike physical money, bitcoin is not actually present in a bitcoin wallet. Instead, they live on the distributed ledger that the Bitcoin network constantly verifies and secures

So how can you own your bitcoin?

You own your bitcoin when you own the private keys allowing you to sign transactions and transfer ownership of that bitcoin to someone else

What is a wallet?

There are two key concepts we describe when using the term “wallet”

- A master private key (like a password, DO NOT SHARE THIS) from which you can generate public keys that you can share with others to receive bitcoin
- Mobile or desktop interface from which you can interact with the Bitcoin network to retrieve your balance, send/receive transactions, and broadcast them to the network

My First Bitcoin
EL SALVADOR

Self-Custodial vs. Custodial Wallets

Wallet Type	Who controls my bitcoin?	Benefits	Risks
Self Custodial Wallets	**The user**	Complete control over funds and transactions, no approval process or account freeze, no corporate or government control, protected against arbitrary confiscation, like keeping money at home.	No recovery if recovery phrase is lost, less customer support, full responsibility falls on the user.
Custodial Wallets	**The third-party provider**	Easy recovery if access is lost, easier customer support	Funds are always connected to the internet, so more vulnerable to hacking and breaches. Custodians control and can freeze accounts.

Self-custodial means that the user holds their own private keys

Custodial means that you are trusting a third party to hold it for you

There are use cases for both types of wallets, but it is important to remember…

NOT YOUR KEYS, NOT YOUR COINS!

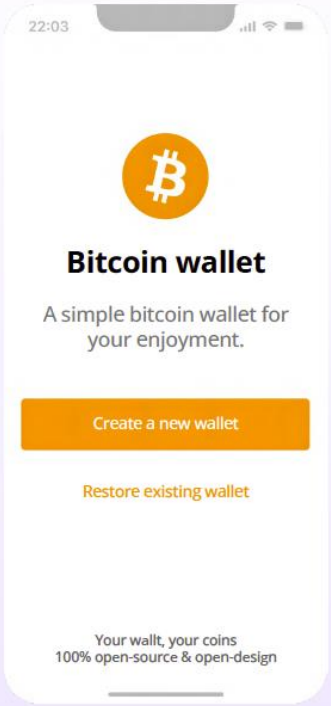
Wallet Type	Description	Advantages	Disadvantages	Example User
Online Wallet	A wallet accessed through a web browser.	Accessible from any device with an internet connection. Easy to use.	Less secure. Can be hacked or compromised.	Someone who needs to access their wallet frequently and doesn't have a lot of funds to store.
Mobile Wallet	A wallet installed on a mobile device.	Convenient. Can be accessed from anywhere.	Can be lost if the device is misplaced, stolen, or hacked.	Someone who needs to make transactions on the go and doesn't have a lot of funds to store.
Desktop Wallet	A wallet installed on a desktop computer.	More secure than online wallets. Can be used offline.	Can be hacked if the computer is infected with malware.	Someone who wants to store a large amount of **bitcoins** and is comfortable with using a desktop computer.
Hardware Wallet	A physical device that stores **bitcoins** offline.	Very secure. Can be used offline.	Funds could be unrecoverable if the device is lost or stolen.	Someone who wants to store a large amount of **bitcoins** and is willing to pay for the added security of a hardware wallet.
Paper Wallet	A physical record of a Bitcoin wallet's private and public keys.	Very secure. Can be used offline.	Can be lost or stolen if the physical record is lost or stolen.	Someone who wants to store a large amount of **bitcoins** and is willing to take added precautions to ensure its security.

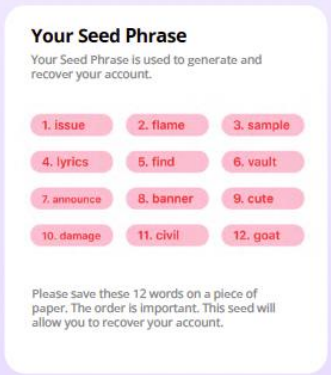
Choosing a Bitcoin Wallet

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

- Security
  - Strong security measures such as 2FA and secure password policies
- Privacy
  - Does the wallet require personal info or allow you to remain anonymous?
- Ease of use
  - Especially for newcomers
- Fees
  - Compare fees to other wallets
- Reputation
  - Research the reputation of the wallet as well as the team that built it
- Control
  - How much control do you have over your private keys?
- Open source
  - Open-source code is important because it allows the community to review what is happening under the hood

My First Bitcoin
EL SALVADOR





Class Exercise: Option 1 — Download a new wallet.

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 bitcoins if you lose access to your wallet.

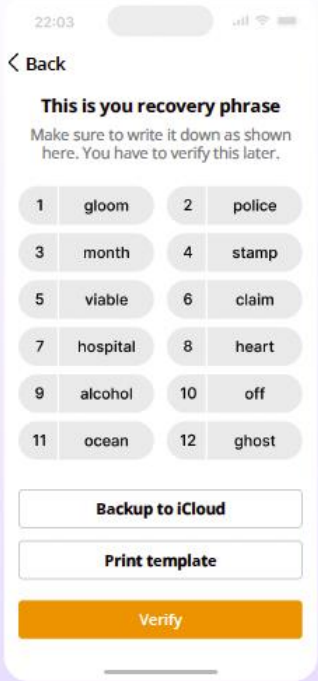
3. You must then confirm that you have actually saved your recovery or seed phrase. To do this, you must enter, in the same order, the words of your seed phrase.
4. As an additional measure of security, some wallets allow you to choose a secure password. Your private key and first Bitcoin address are automatically created for you by your wallet.

Think of your public key as your email address — you want to share this with others so that they can send you bitcoins — or, in the case of an email address, an email.

Think of your private key 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 bitcoins. Transfer bitcoins to your wallet. With a self-custodial wallet, you cannot always buy bitcoins directly with fiat, so you might need to purchase and transfer them from an exchange first.

Try out one of these exercises to become more comfortable with bitcoin wallets!



Class Exercise: Option 2 - Restore a 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:

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" message when your wallet has been successfully imported.

Receiving and Sending Transactions

A bitcoin transaction is a transfer of ownership of existing bitcoin to a new owner

When a transaction is confirmed, all the nodes in the network update their local copy of the public ledger to reflect the transfer of ownership

A transaction can be sent only when the sender signs a message with their private key, this signals to the network that the sender does in fact own that bitcoin and can send it to the recipients receive address

LEDGER

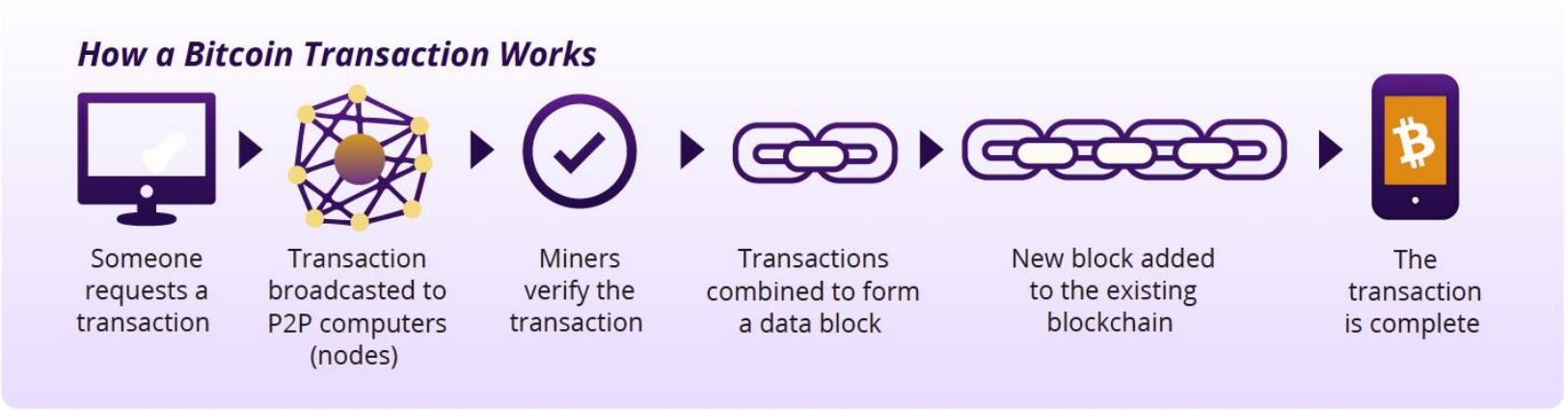
Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.50
Robert	2.00
Eliana	1.75
Daniel	5.25

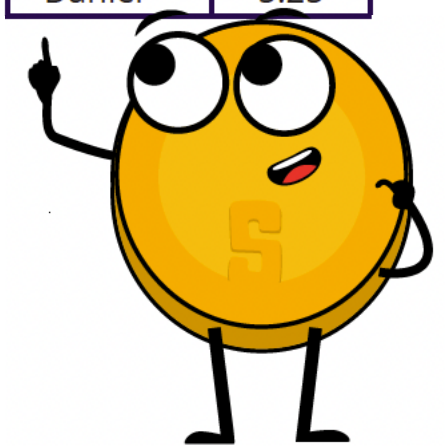
Bitcoin Transaction Request Message
Jim sends 0.50 BTC to Eliana

Jim ▸ Eliana 0.50 BTC

LEDGER

Account Owner	Value
Sam	2.50
Adam	3.00
Michael	6.00
Jim	1.00
Robert	2.00
Eliana	2.25
Daniel	5.25

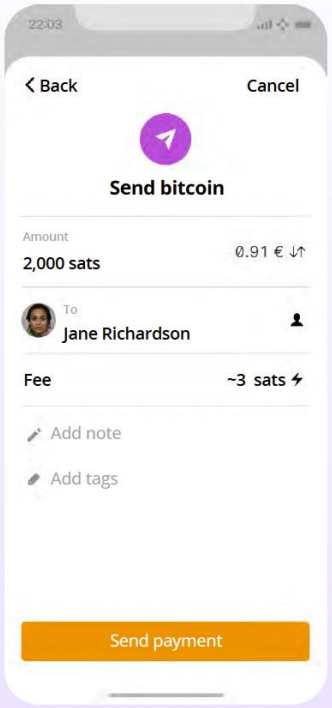




My First Bitcoin
EL SALVADOR

Here is an example of how sending/receiving a bitcoin transaction might look on a mobile interface

Sending Bitcoin Transactions:



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

1. Open your Bitcoin wallet. An 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 number of bitcoins 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 you double-check the transaction details one more time to ensure that you are sending the correct amount of bitcoins 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 bitcoins 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 bitcoins. However, on-chain transactions are slower and can be significantly more expensive than other options, such as the Lightning transactions we will discuss in Chapter 8.

Receiving Bitcoin Transactions:

To receive bitcoins, 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" bitcoins.

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 bitcoins.
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.

Key Players in a Bitcoin Transaction

- Senders and receivers are the parties who wish to transact with each other
  - Senders create and broadcast transactions
  - Receivers receive and verifying transactions
- Nodes validate transactions and store a complete copy of the blockchain
  - Nodes validate transactions in accordance with consensus rules
- Miners are responsible for adding new transactions to the blockchain
  - Miners earn a block subsidy and transaction fees as a reward for real life proof-of-work (solving cryptographic puzzles)

My First Bitcoin
EL SALVADOR

Saving in Bitcoin

Bitcoin is a way to safeguard your money against inflation and protect it from being controlled by anyone else

The type of money you choose to save in is one of the most important decisions you can make.
Choosing wisely allows you to build a better future for yourself and your family

When stored properly, bitcoin is the only form of property no one can take away from you

Don’t Trust, Verify

Always remember, there are no leaders in bitcoin. There are no heroes. You should never blindly follow someone else’s claims. Everyone here plays by the same rules, there are NO exceptions.

You should always question what you’re being told and verify it for yourself. This is the best way to protect yourself from losing your bitcoin.

757btc.org