Digital Signatures and Keys

FinTech

Lesson 19.2

Class Objectives

- Summarize asymmetric and symmetric cryptography and how they can both increase security.
- Describe the process in which digital signatures authorize blockchain transactions.
- Evaluate the roles of hot and cold wallets.
- Detail how wallets use public- and private-key pairs and store cryptocurrency.
- Articulate the role of Bitcoin improvement proposals (BIPs), specifically BIP-39 and BIP-44, and how to use them to generate mnemonic phrases.
- Develop an Ethereum account by using BIP-44, BIP-39, and Python.
- Use mnemonic phrases and Web3.py to create a verifiable transaction.
- Create, sign, and send a transaction using your Ethereum account.


WELCOME

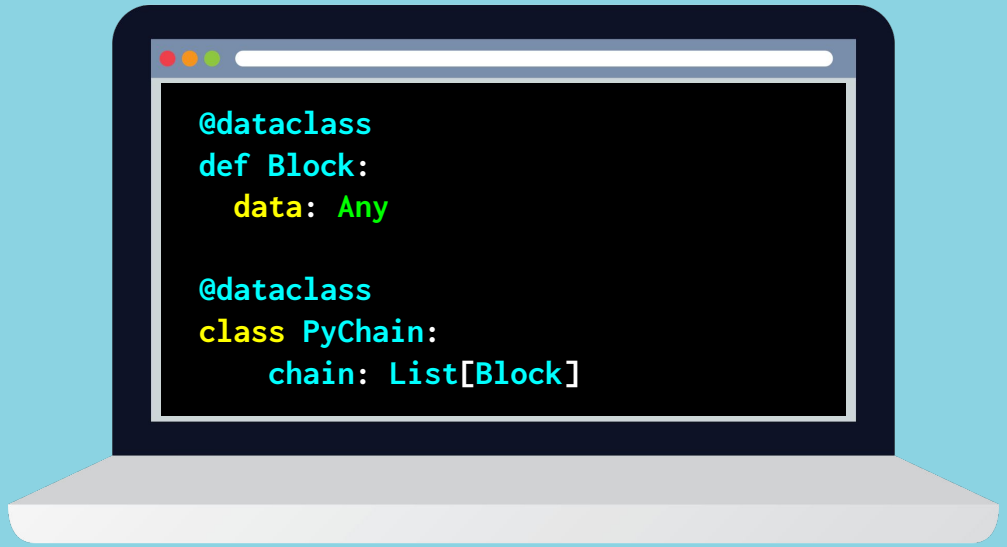
Let’s begin by recapping the previous unit and lessons.

Recap

In the previous unit, you learned how to build a blockchain-based ledger system from scratch. In your `PyChain`, each block on the chain stored data for the ledger.

Blockchain blocks can store any type of data, from the transfer of cryptocurrency funds to the text of a complex legal document, or even a simple sentence such as “Jeremy owes Sue $20.”

Regardless of content, each of these records represents a basic blockchain transaction.

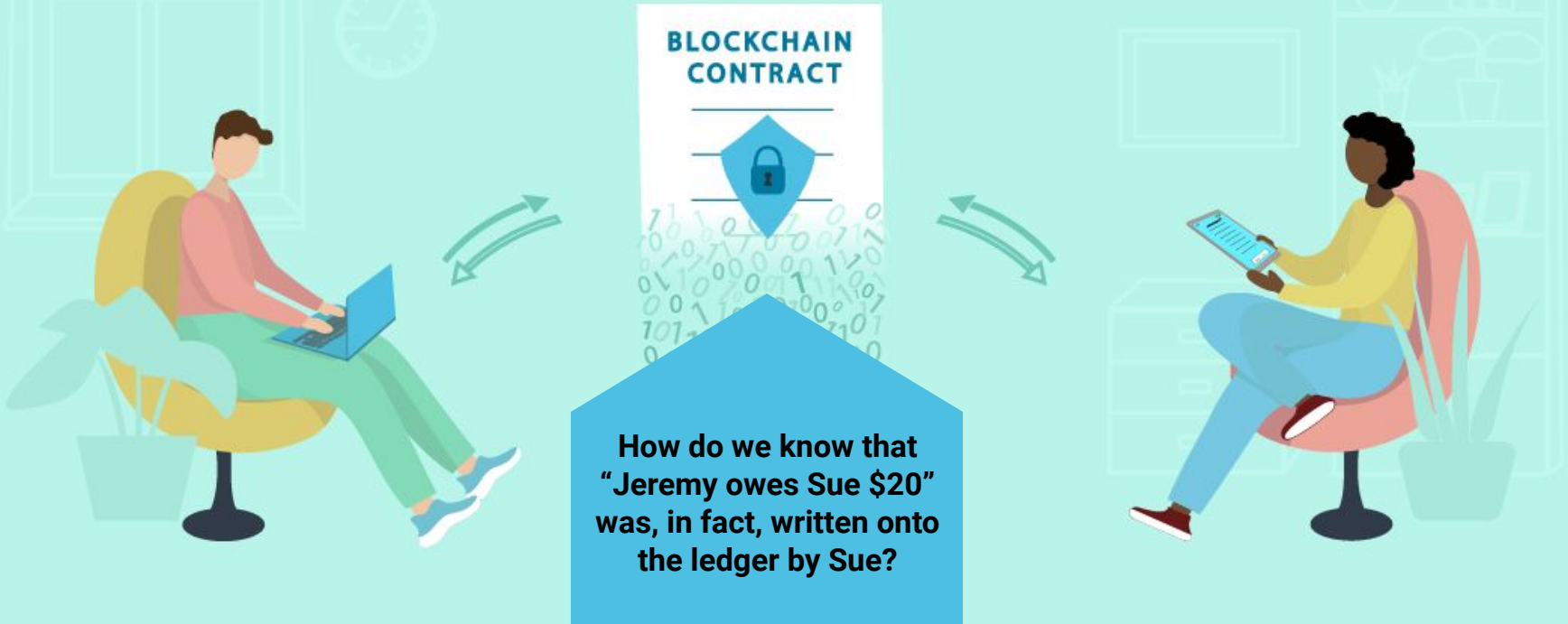


The lessons have covered how to execute and verify such transactions.

But there’s one question we haven’t considered.

Digital Signatures

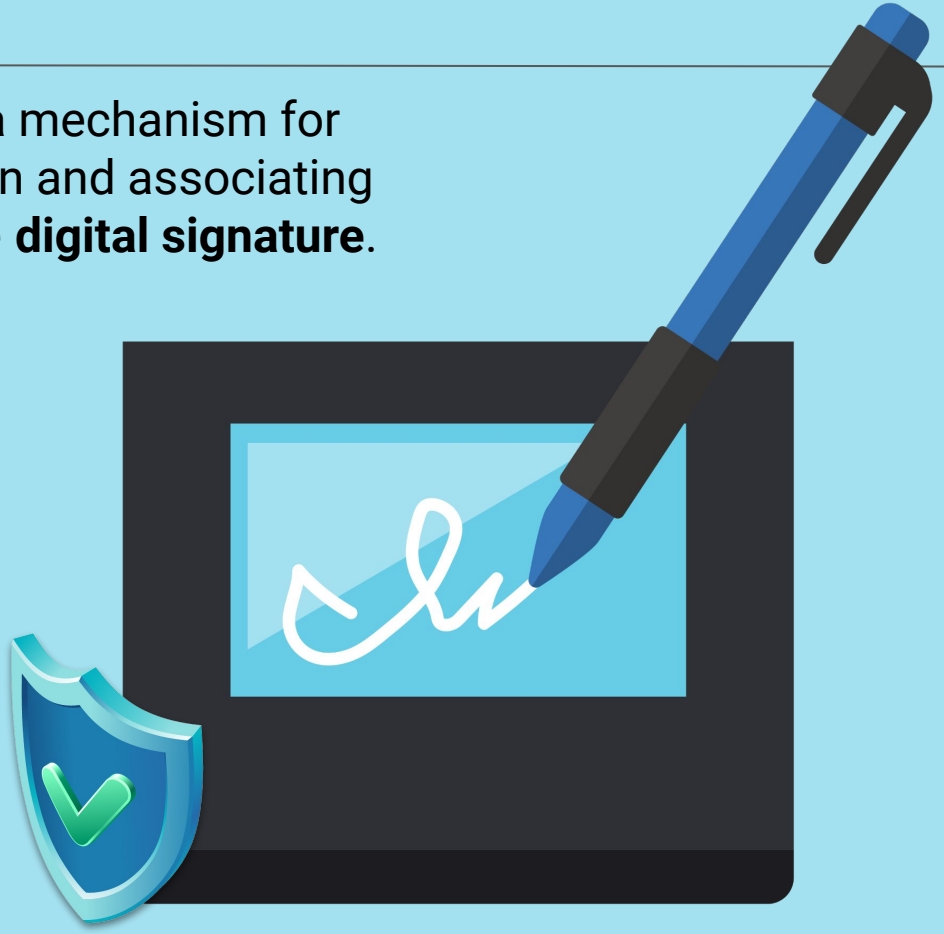
If anyone can create a transaction and store data on the blockchain (as long as they pay the transaction fee), how do the ledger's participants know who has added which transactions to the ledger?



Digital Signatures

Blockchain developers have created a mechanism for identifying participants in a blockchain and associating those identities with transactions: the **digital signature**.

- A participant's digital signature proves that they authorized a given transaction on the blockchain.
- Like most features of a blockchain, digital signatures are designed to make the blockchain system more secure and verifiable.



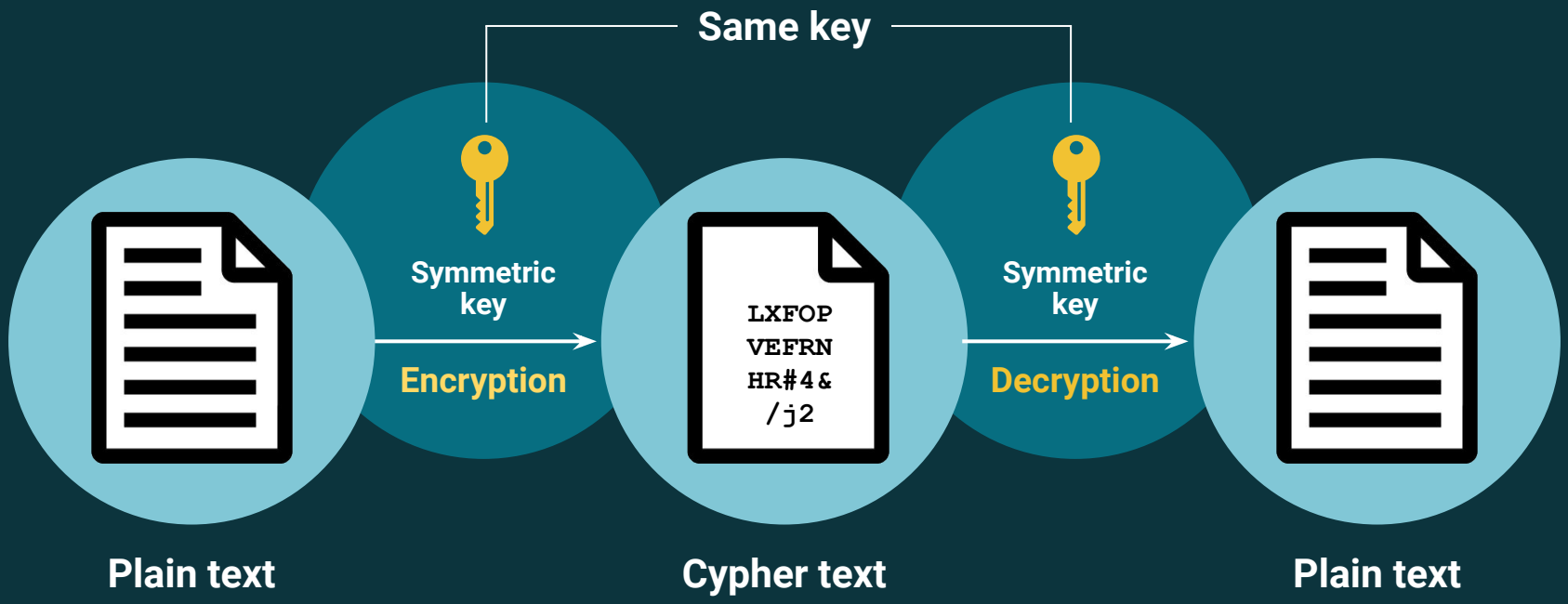
Some Major Companies Using Cryptocurrency

Symmetric and Asymmetric Cryptography

Let’s explore the encryption technology that powers digital signatures.

Symmetric Cryptography

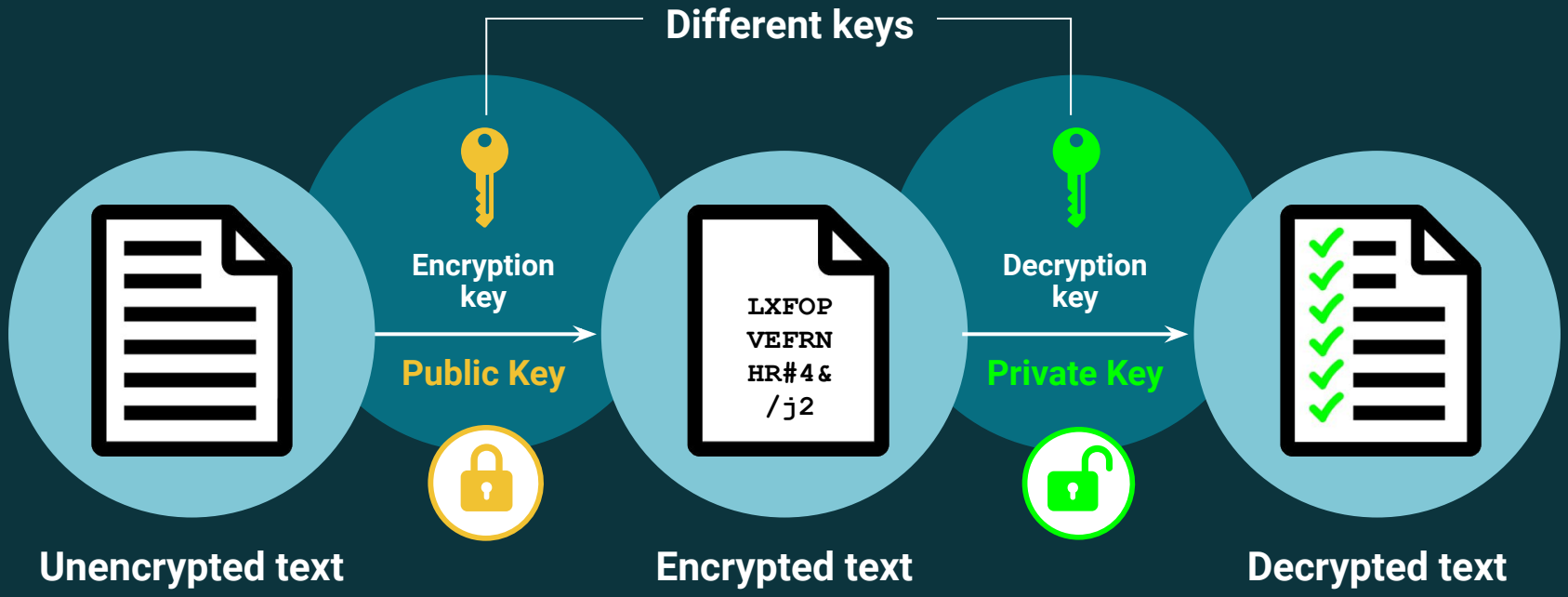
Symmetric cryptography means that for one lock, there is **one key**.
This one-to-one relationship provides symmetry.



(Source)

Asymmetric Cryptography

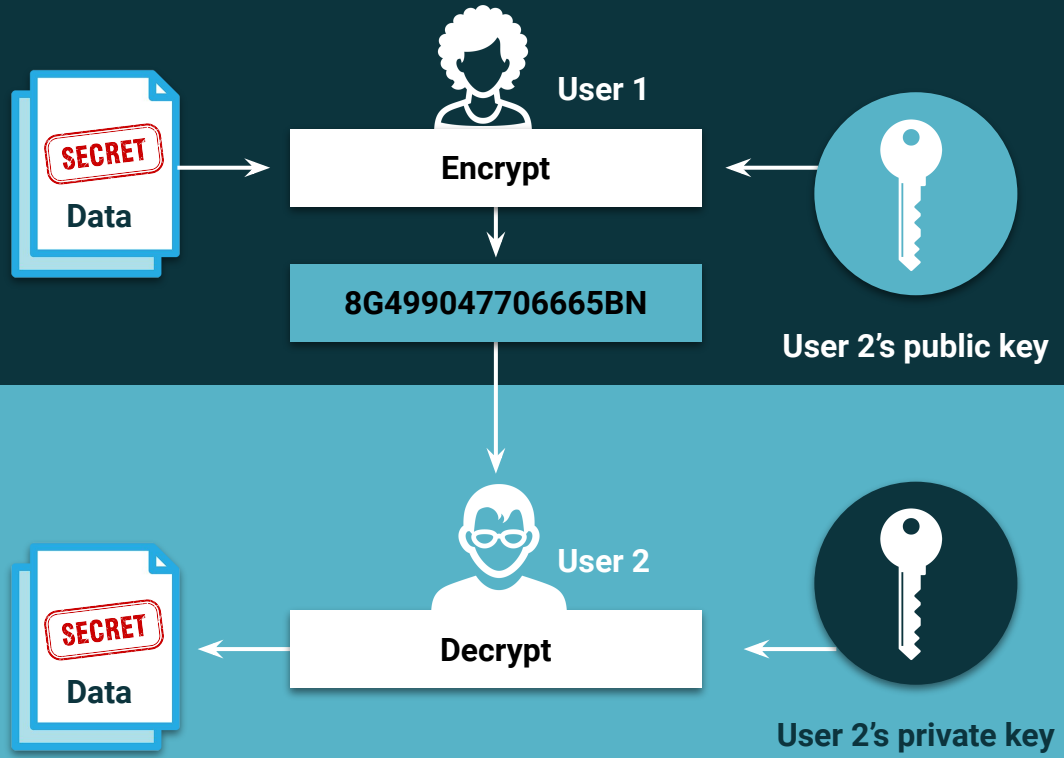
Asymmetric cryptography splits this key into a **key pair**. Each key pair includes a **public key** and a **private key**.



(Source)

Asymmetric Encryption

This diagram depicts the **asymmetric encryption process** with a public-private key pair.



Asymmetric cryptography makes it much harder for malicious hackers to read data by getting a hold of a key, because you never have to send a private key over a network or share it with anyone.

Activity: Secretbox Demo

In this activity, you will encode a message with the Secretbox created by TweetNaCl.js.

Suggested Time:

10 minutes

Time's Up! Let's Review.

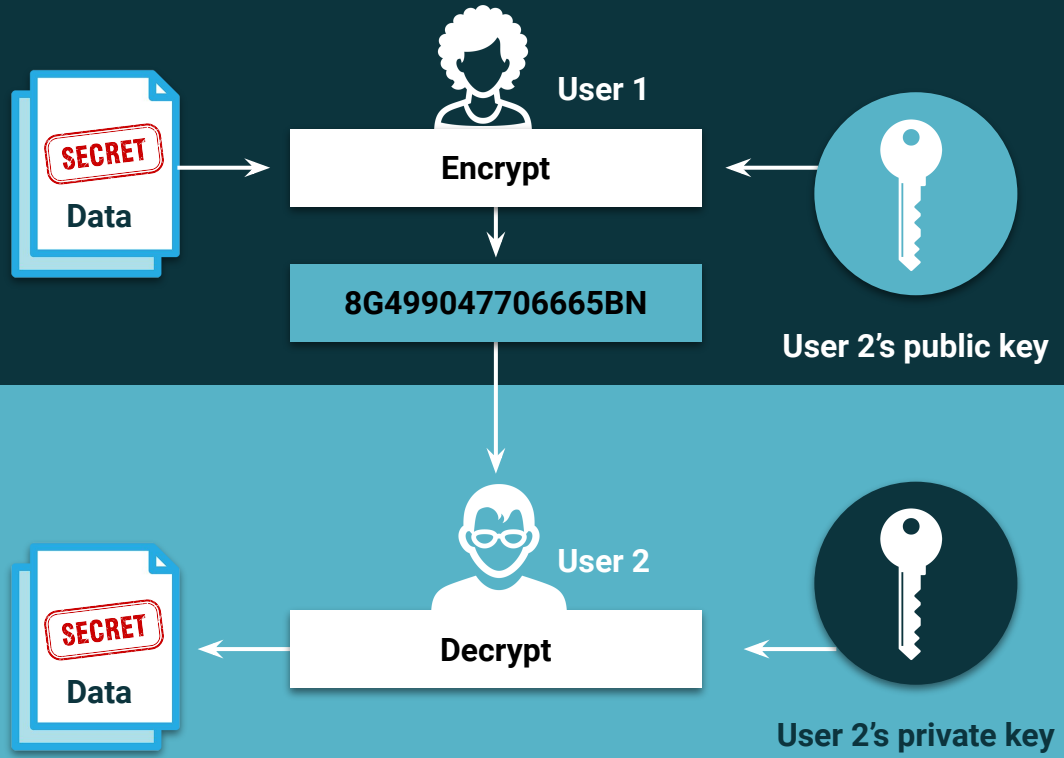
Questions?

Signatures and Wallets

Asymmetric Encryption

Blockchain leverages public-private key pairs to secure communications or transactions using asymmetric cryptography.

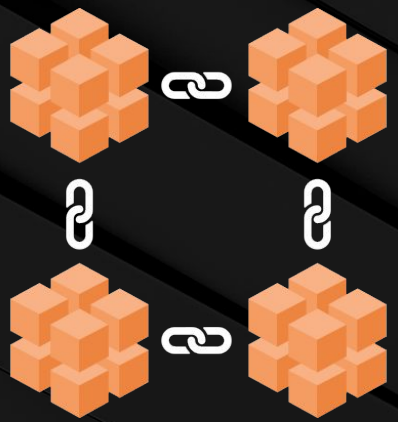
The user's private key is used to create a digital signature that secures all blockchain transaction.



Digital Signatures

Maybe you've signed a digital document or used another digital document-signing service before.

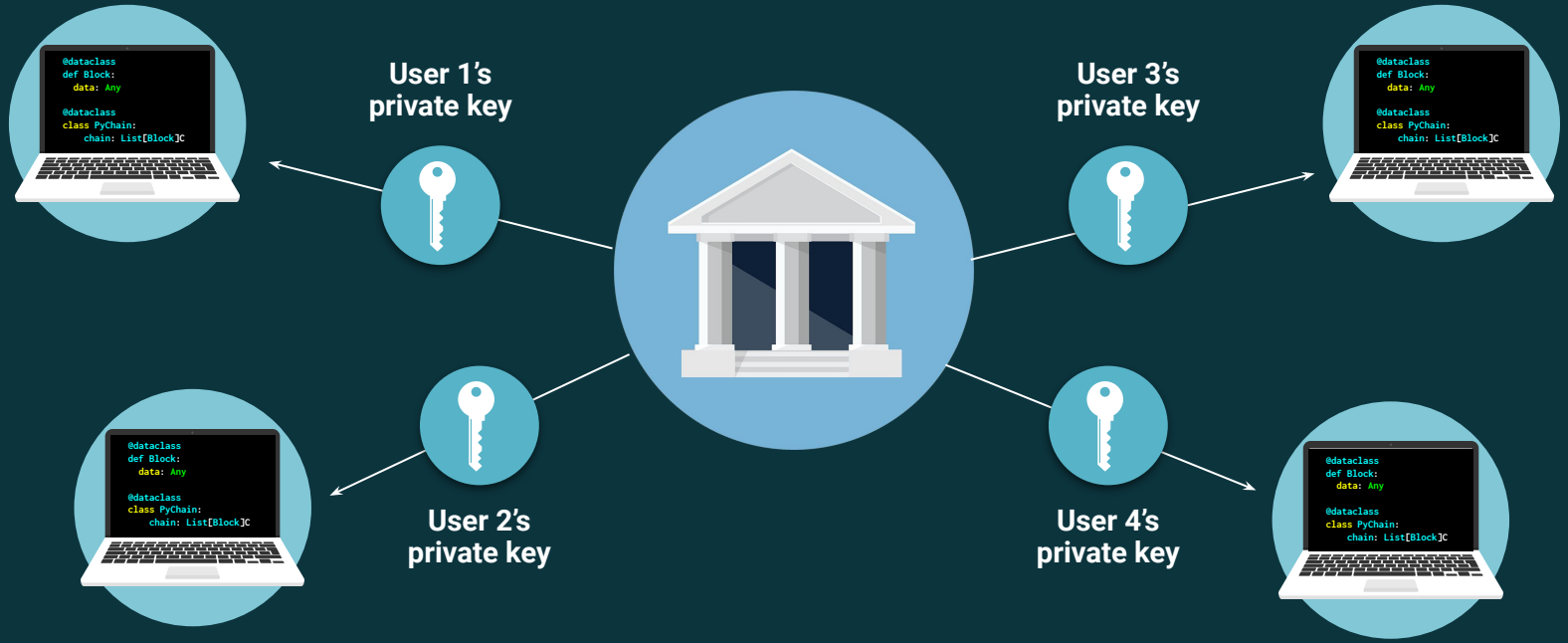
These services use cryptography to create digital signatures that prove that a document or transaction has been authorized by the proper individual(s) and that the signed document has not been tampered with.



Similarly, blockchains use asymmetric cryptography to generate a digital signature, or a public-private key pair, for each participant.

Private Key

Each participant on the blockchain has one private key. This private key is used to sign documents, messages, or transactions that they send to the blockchain—in other words, to **authorize** transactions.



Private keys should never be shared with anyone.

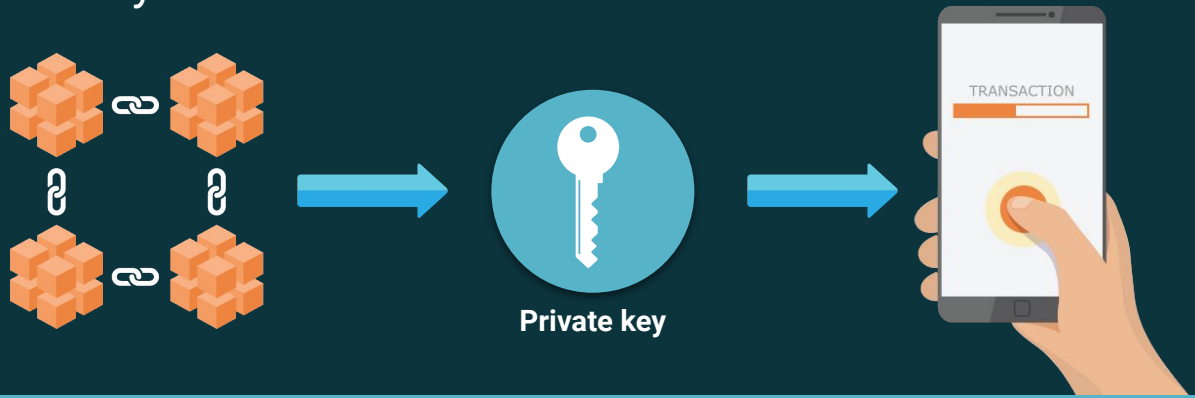
(Just as you would never share your bank account PIN with anyone.)

Sharing your private key will put your wallet at risk for being emptied by bad actors.

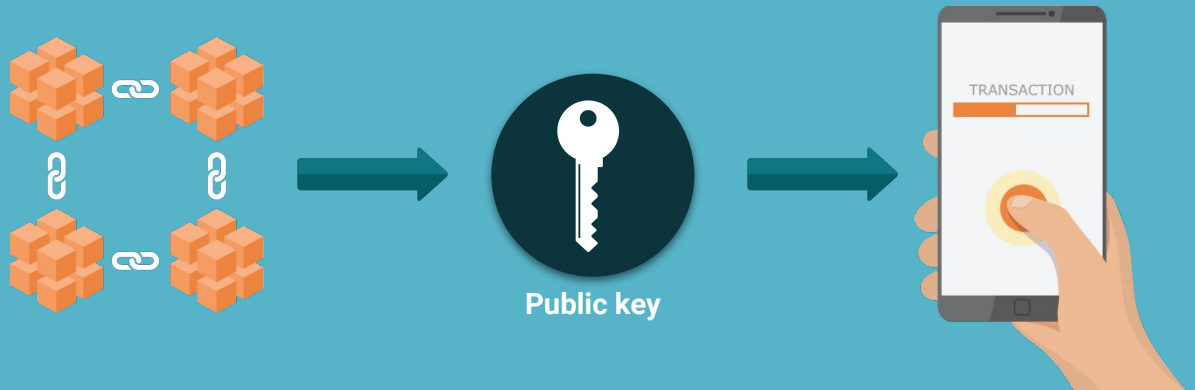
Private vs. Public Keys

Cryptography is used in almost every industry that uses computers.
In the context of cryptocurrency:

Use your
private key
to send funds.



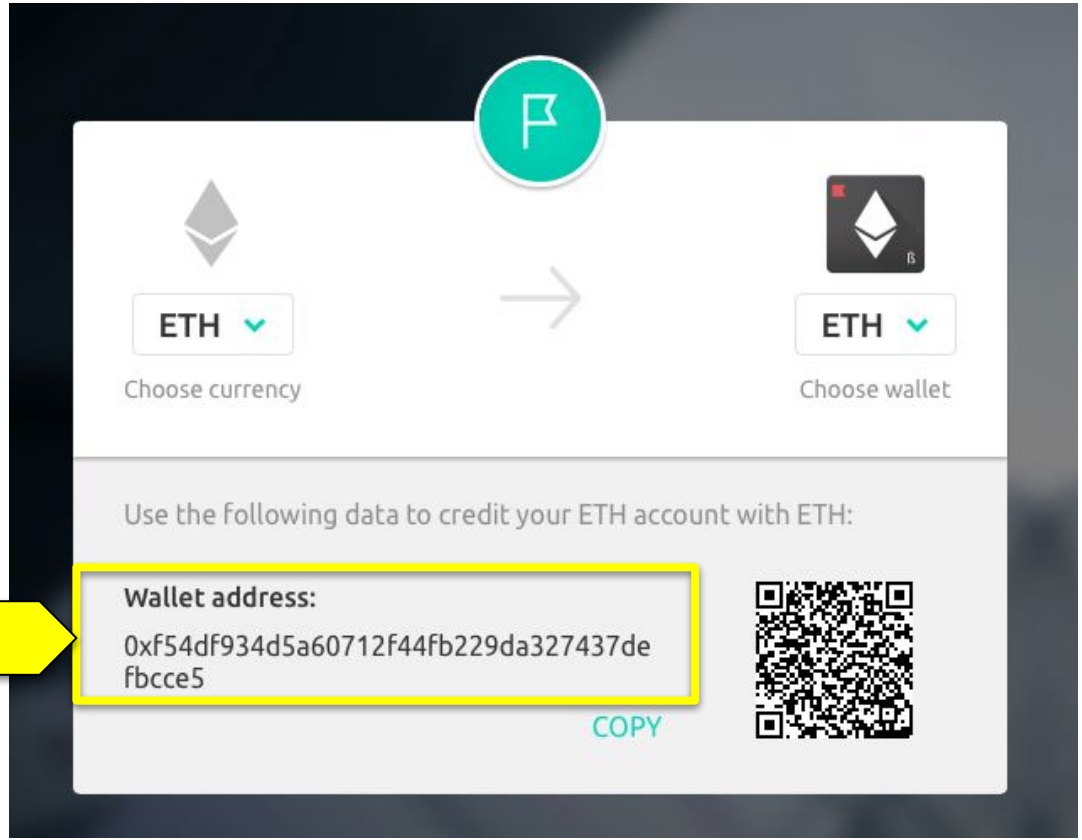
Use your
public key
to receive funds.



Private vs. Public Keys

Recall from the previous lesson that every blockchain participant has an account address, like a bank account number, where other participants can send funds.

On Ethereum blockchains, a participant's account address is a shortened version of their public key.



Private vs. Public Keys

It is common that a blockchain participant has one private key and one associated public key, but it's possible to associate more than one public key with a given private key.

Some blockchain participants choose to associate multiple public keys with their private key in order to increase privacy.

It's also possible for one blockchain participant to use multiple private keys. Again, some individuals do this to increase privacy and data security.

For this lesson, you will create your blockchain accounts with one private key and one associated public key.

Private vs. Public Keys

The same private key can be used across multiple blockchains if they use the same protocols. For example, a blockchain participant could use the same private key for their accounts on both Bitcoin and Ethereum.

Wallets

A **cryptocurrency wallet** is a software program or physical hardware device that securely stores and manages a blockchain participant’s payment information.

Wallets

A blockchain participant uses their wallet to:

Store their private key

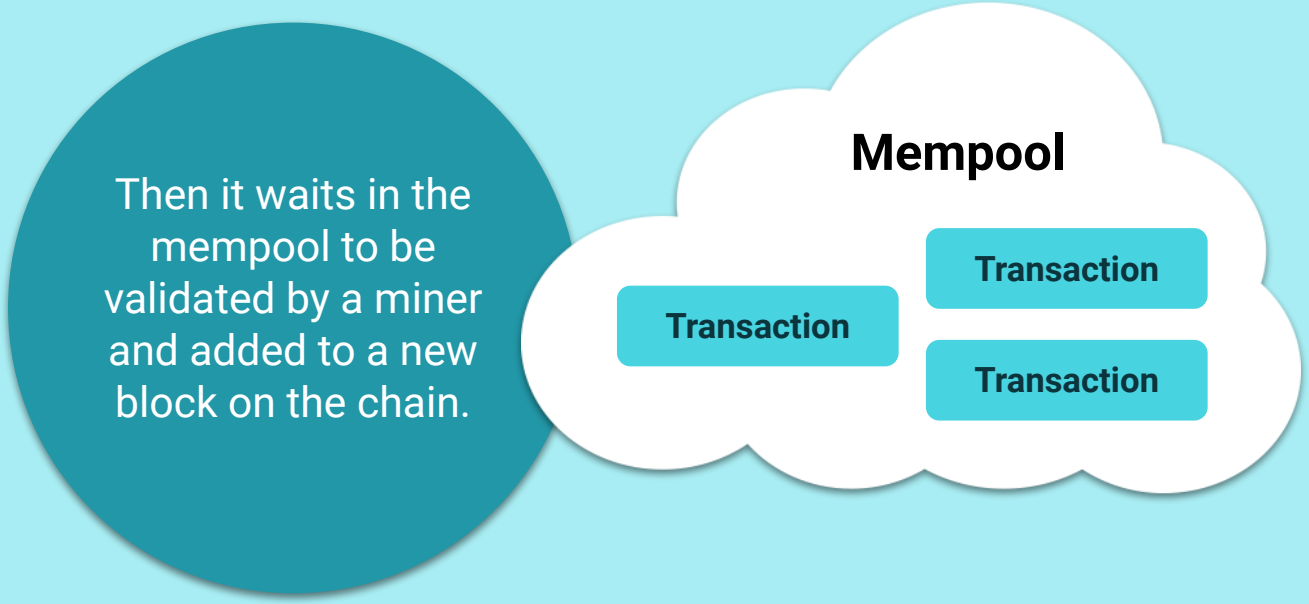
Confirm their cryptocurrency balance

Create cryptocurrency transactions

Authorize the transactions using their private key

Wallets

Once a transaction has been created and authorized from within the wallet, it is sent to the blockchain.



Wallets

Some digital wallets can only hold the information for a single cryptocurrency. But multi-currency wallets exist that can accommodate several cryptocurrencies.

In short, a digital wallet allows you to both spend your cryptocurrency and verify your ownership of it.

Digital Wallet Providers

These digital wallets are software programs that you download to your computer or smartphone. You can also code your own wallet, which we'll do later in this lesson!

Wallets have various levels of security, depending on how they're constructed and how they store keys.

Hardware Wallets

Hardware wallets store the cryptographic keys inside of a special chip.

Some hardware wallets are **cold wallets**.

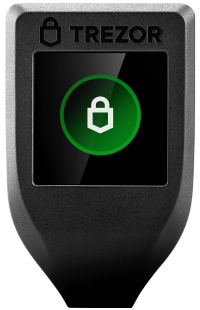
This type of wallet rarely, if ever, connects to the internet.

Hardware Wallets

Providers of hardware wallets include:

The keys a hardware wallet stores are completely disconnected from the digital world, except in rare moments. This makes these wallets extremely difficult for bad actors to tamper with.

[Ledger]

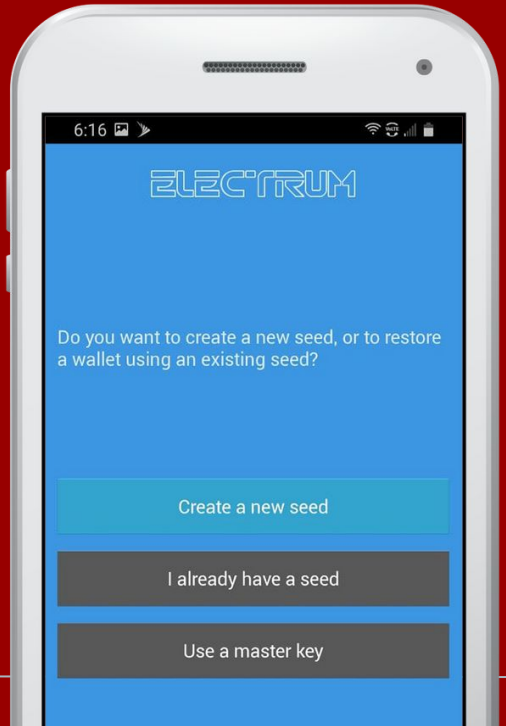


[Trezor]

[KeepKey]

A hot wallet can be:

A software application on your phone or computer



A hardware wallet that connects to the internet via the USB port on your computer

(Source)

Hot wallets are **less secure** than cold wallets because their internet connection can present opportunities for bad actors to access the programs, if they’re not properly secured, and gain access to the stored digital keys.

Hot Wallet

- Software
- Often or always connected to the internet
- Easier to access account information
- Less secure

Cold Wallet

- Hardware device
- Rarely connected to the internet
- More difficult to access account information
- Extremely secure

Generating a Private Key

The procedure that we'll use to generate our mnemonic seed phrase, which will used to generate our private key, involves two different BIPs.

A **Bitcoin Improvement Proposal (BIP)** is a proposed standard that would current Bitcoin protocols or processes.

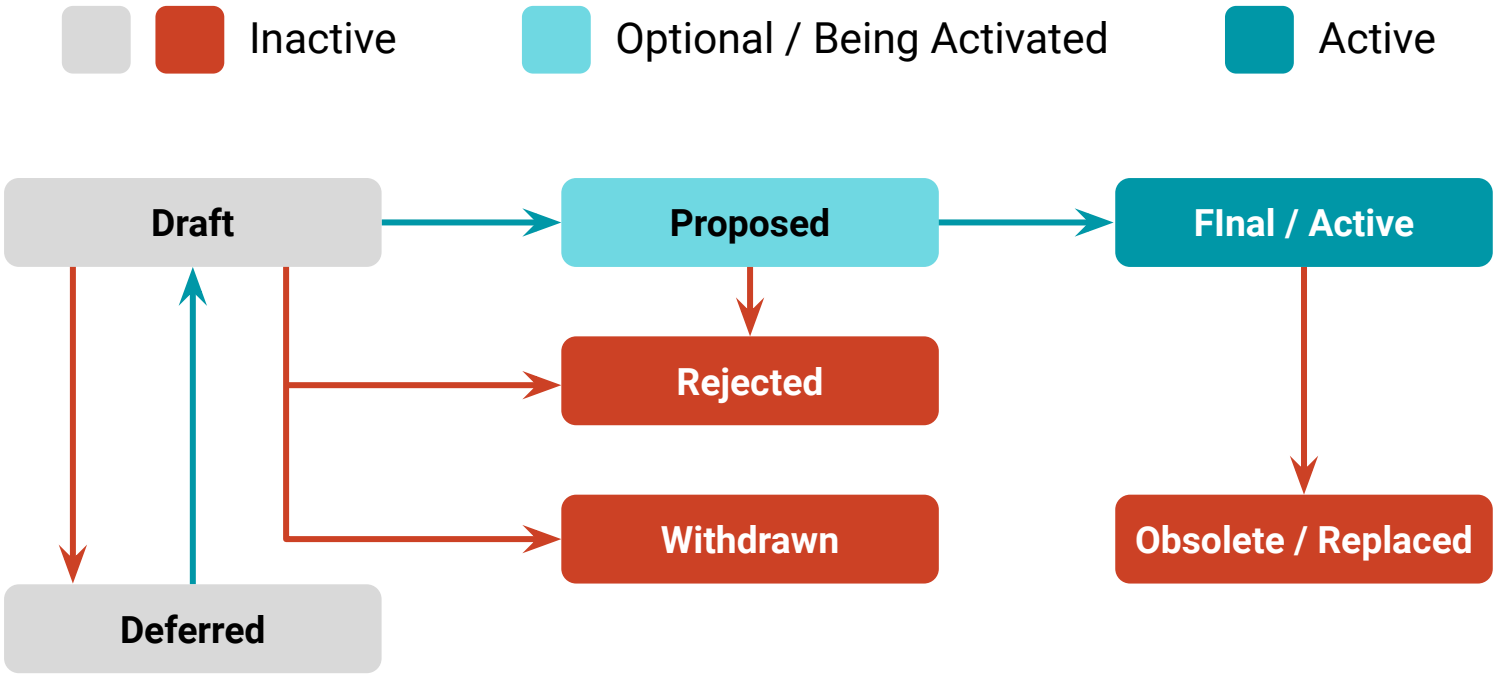
Bitcoin Improvement Proposal (BIPs)

New BIPs are voted on by the Bitcoin blockchain community. If a majority favors the BIP, it is adopted and implemented.

BIPs can include changes to the process of validating transactions within the Bitcoin ecosystem, or improvements to the core process of running the Bitcoin ecosystem.

Like many aspects of Bitcoin, many BIPs are also adopted by other blockchains, including Ethereum.

Bitcoin Improvement Proposal (BIP) Process



(Source)

Bitcoin Improvement Proposal (BIP) Process

The two BIPs used today have been widely adopted and will help us generate our Ethereum private key.

BIP-39

BIP-39 sets a standard for using a **mnemonic phrase**, or **seed phrase**, which serves as a backup that can recover your private key if your wallet is compromised, lost, or destroyed.

BIP-44

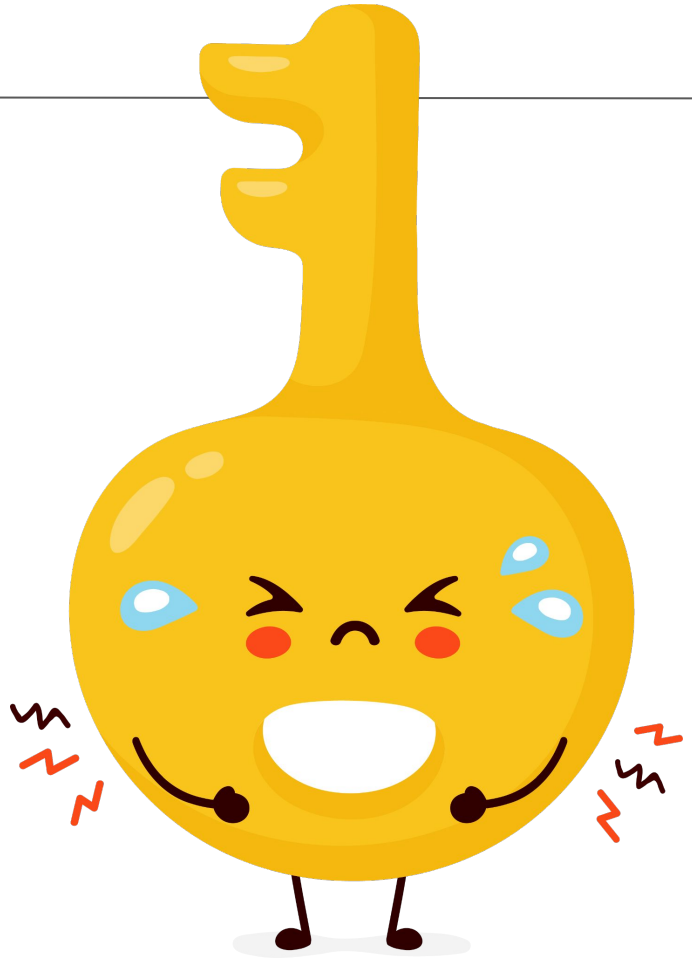
BIP-44 uses a **mnemonic seed phrase** to derive **keys**, including public- and private-key pairs. This allows the user to avoid storing and generating new keys for each use.

A **mnemonic seed phrase** is a string of randomly selected words that is used to generate a private key.

Mnemonic Seed Phrase

Generating a private key from a random string of words enhances the security of the private key by making it harder to guess.

It also makes it harder to lose your private key.



(Source)

Mnemonic Seed Phrase

Because humans tend to be bad at generating randomness when selecting their own words, BIP-39 has become one of the most common standards for creating seed phrases.

Letting the wallet software generate the 12- or 24-word seed phrase means that the participant's only responsibility is to write the phrase down and keep it somewhere that's safe—both from being lost and from malicious hackers.

Mnemonic Seed Phrase

BIP-39 includes a list of **2,048 words** that can be included in seed phrases.

To generate a seed phrase, a digital wallet typically selects either **12 or 24 words** from this list at random.

This is an example of a 24-word seed phrase created by using BIP-39:

1	toe	7	little	13	globe	19	cousin
2	miss	8	wink	14	thank	20	vibrant
3	arrive	9	any	15	clump	21	hockey
4	bonus	10	knee	16	connect	22	wave
5	gallery	11	exhaust	17	second	23	fragile
6	fan	12	below	18	bicycle	24	cricket

Mnemonic Seed Phrase

The first step is to derive a private key from a seed phrase by using BIP-44.

BIP-44 is simliar to BIP-39.

In order to derive a private key from our seed phrase, we can use another BIP, BIP-44.

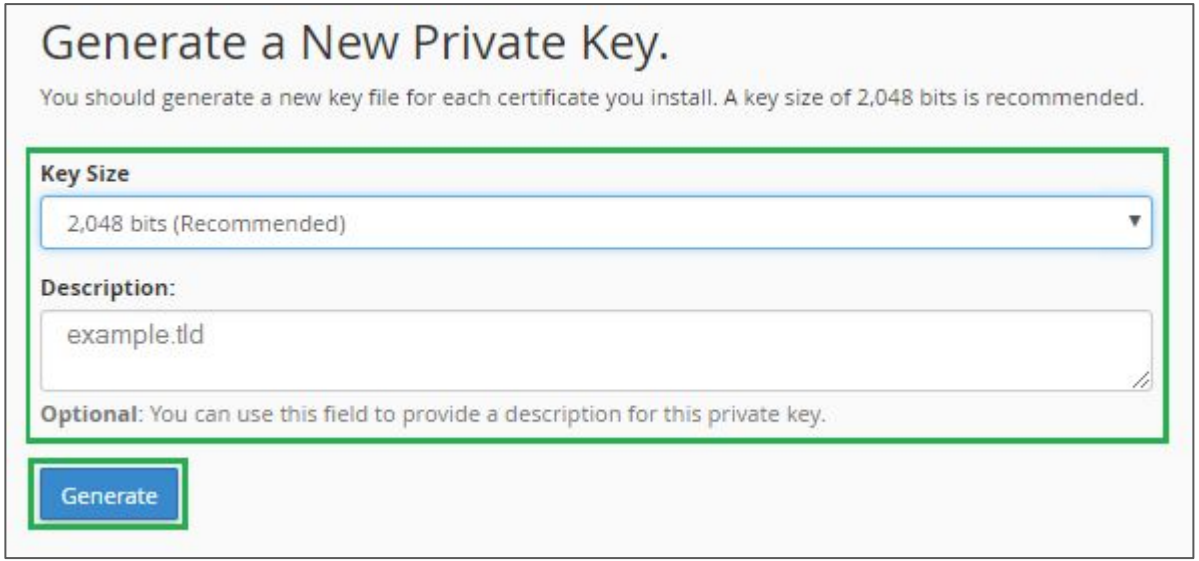
This BIP will convert the seed phrase to a corresponding private key that we can use to authorize transactions on a blockchain network.

Remember: Blockchain participants store private keys in their wallets. Like BIP-39, BIP-44 was designed for hierarchical deterministic wallets (HD wallets).

Mnemonic Seed Phrase

HD wallets automatically generate the public-private key pair from the seed phrase, rather than having the user do it manually.

- Most blockchains now use BIP-44 as the standard for generating public-private key pairs.
- BIP-44 has been widely adopted because it allows a single wallet to handle multiple coins, multiple accounts, and even multiple public-private key pairs.



Questions?

Creating an Ethereum Account

Suggested Time:

25 minutes

Time's Up! Let's Review.

Questions?


Break

Activity: From Mnemonic to Ethereum Account

In this activity, you will use the mnemonic and BIP-44 packages as well as the Web3.py library to generate a wallet instance and a secure public-private key pair.

Suggested Time:

20 minutes

Time's Up! Let's Review.

Questions?

Signing and Verifying Messages with Web3.py

Suggested Time:

20 minutes

Activity: Signing Ethereum Transactions

In this activity, you will use the Web3.py library to sign and authorize messages by using your public-private key pair.

Suggested Time:

20 minutes

Time's Up! Let's Review.

Questions?

Summary

Today, you learned:

Asymmetric cryptography and how it applies to blockchain

How to use BIPs, and how they impact the blockchain

How to sign and send transactions


The End