CryptoCurious

Crypto Wallets and Basic Security

Presented by:
Shirley McPhaul

Sponsored by:
DLTX

CryptoCurious

Today's Agenda:

- Introduction
- "Crypto Wallets" 101
- Different types of wallets
- Protect Your Crypto Assets from bad actors and yourself.
- Conclusion

CryptoCurious

By the end of today's webinar,
we will have answered:

- What is a "crypto wallet"?
- Why do I need a wallet in the Web 3.0?
- What is the difference between a "hot" and a "cold" wallet?
- How can I protect my crypto-assets from bad actors (and myself)?

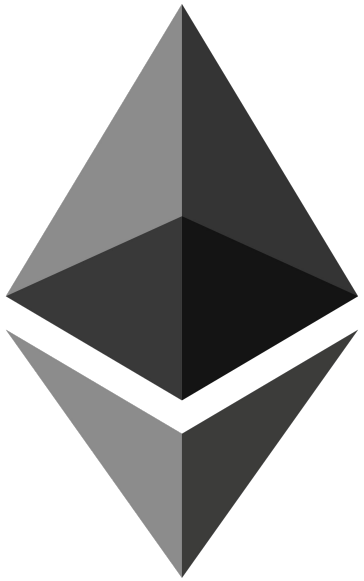
Introduction

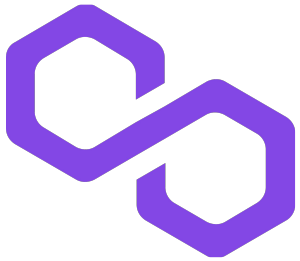
¡Hola!

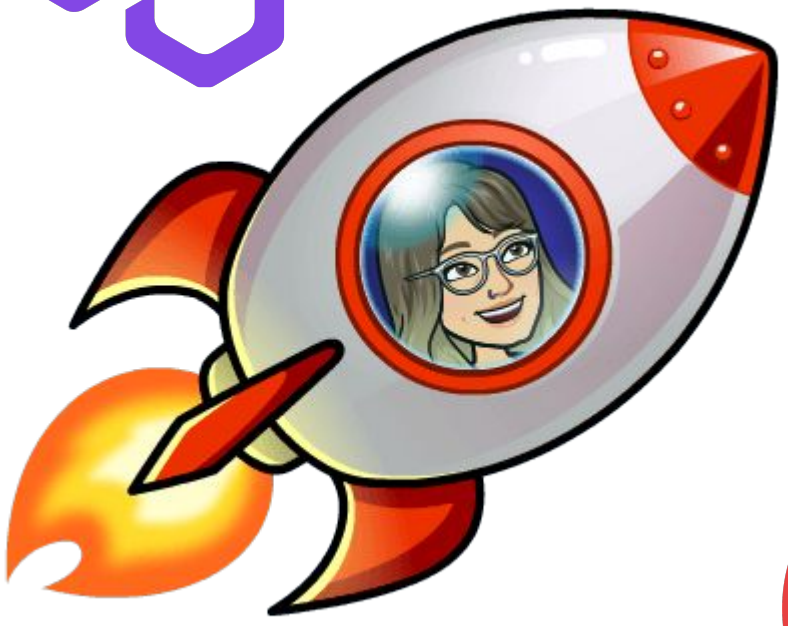
My name is Shirley

Introduction

I've onboarded and experimented on several blockchains







Introduction

I've learned that

- active experimentation and exploration is the most effective way to become proficient within this space.
- some concepts are too alien from our regular experience to be graspable only through theory.
- prioritizing the "why" rather than the "what" helps in the process of understanding the whole space.

CryptoCurious

Crypto Wallets 101

What is a “crypto wallet”?

What is a “crypto wallet”?

A. A digital tool that holds your crypto.
B. An application that secures your crypto assets
C. A product that lets you manage Web 3.0 accounts by enabling access to your account’s balance, send transactions, interact with DApps, etc
D. I have no idea

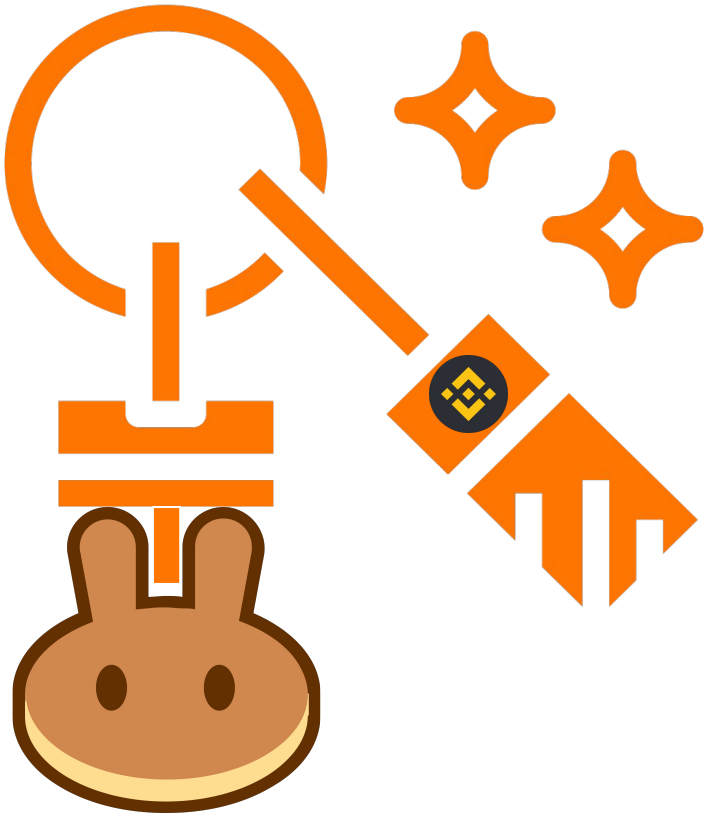
What is a “crypto wallet”?

“A wallet is a product that lets you manage your (Insert Blockchain Name Here) account. It allows you to view your account balance, send transactions, and more.”

- Ethereum.org/en/wallets

What is a “crypto wallet”?

This is why it may be more helpful to think about your crypto wallets as **keychains**, rather than a traditional wallet.

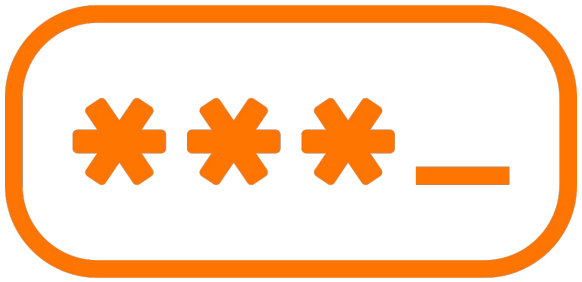


What is a “crypto wallet”?

A “crypto wallet” holds your “keys”, allowing you to transact with Web 3.0 applications.

Private Keys

Your Password/Seed Phrase



Public Keys

Your “Wallet address”

What is a “crypto wallet”?

This begs the question:

If not in my wallet, where’s my crypto being stored? 🤔

- When you transact in any blockchain, all you are doing is executing smart contracts.
- When you purchase cryptocurrencies, a smart contract assigns the amount purchased to your account.
- Your wallet shows your account’s balance, but no “money” is being moved. Not necessarily.

CryptoCurious

Crypto Wallets 101

Why do I need a “Crypto Wallet”?

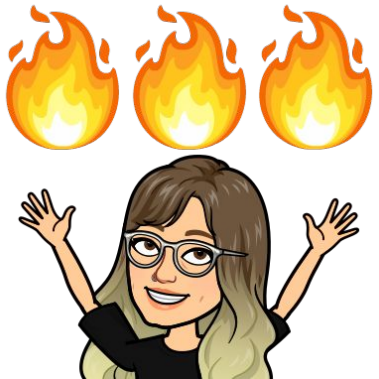
Why do I need a “Crypto Wallet”?

Why do I need to “hold my keys”?

- Navigating a decentralized internet requires YOU (the user) to have the autonomy to make decisions without having to consult an institution for permission.
- By “holding your keys” and assuming full responsibility over your assets, you are given both control and freedom over how you can use them.

Pros

- Complete control over your assets



Cons

- Complete control over your assets

Why do I need a “Crypto Wallet”?

What does “complete control over your assets” mean?

- You can decide how your assets work for you.

- You are 100% responsible for your asset’s security
- Most decentralized projects don’t have customer service or any effective ways to help you if something goes wrong.
- The crypto market is very loosely regulated (for now), making it easier for bad actors to take advantage of new user’s ignorance.
- Forgetting your password or losing access to your “keys” could represent the permanent loss of your assets.

Why do I need a “Crypto Wallet”?

But, what if you don’t want this responsibility?

- That’s okay! Loads of people don’t

If your sole interest is to invest in cryptocurrencies, can simply use “Centralized Exchanges” and let them “hold your keys” for you.

- Coinbase
- Binance.US
- Kraken

However…
If you want to explore the emerging world of decentralized applications, you will need a “Crypto Wallet”.

CryptoCurious

Crypto Wallets 101

Types of “crypto wallets”

Types of Crypto Wallets

Two Ways to Categorize them

In terms of their materiality

Software Wallets

Hardware Wallets

Paper Wallets

In terms of how they operate

Hot Wallets

Cold Wallets

Types of Crypto Wallets

Software / Hardware / Paper

Always connected to the internet

Hot Wallets

- **Web Wallets**
  - Metamask
- **Desktop Wallets**
  - Exodus
- **Mobile Wallets**
  - TrustWallet

Can be disconnected from the Internet

Cold Wallets

- **Ledger**
- **Trezor**

Don't need internet

- **Printed QR codes**
- **A notebook**
- **100% Not recommended**

Types of Crypto Wallets

Software / Hardware / Paper

Hot Storage

- Web Wallets
- Desktop Wallets
- Mobile Wallets
- Exchanges

Cold Storage

- Ledger
- Trezor

What about Exchanges?

Centralized | Decentralized

Hot Storage

"Not your keys, not your crypto"

- In theory, exchanges should NOT be used for storing your cryptocurrencies
- In practice, a lot of people choose to because by doing so they can receive some type of yield or incentive.

You are 100% responsible

- Decentralized Finance (DeFi) platforms offer tools to manage your capital in ways it hadn't been possible for individuals before.
- They offer the ability to put your assets to work for you in life-changing ways
- It is extremely risky
- While "providing liquidity" or "staking" your assets in a decentralized exchange, you could be exposing yourself to rugpulls.

Types of Crypto Wallets

Which option is best?

Software / Hardware / Paper

Hot Wallets

- **Web Wallets**
- **Desktop Wallets**
- **Mobile Wallets**

Less secure, more convenient

Cold Wallets

- **Ledger**
- **Trezor**

More secure, not as convenient

- **Printed QR codes**
- **A notebook**
- **100% Not recommended**

Types of Crypto Wallets

What is the general recommendation?

- **Store any crypto you're holding long term in a Cold Wallet**
- **Never leave crypto in exchanges**
  - **If you do, understand the risk, and NEVER put all your crypto in a single platform at a time.**
- **Have multiple wallets to mitigate risk**

CryptoCurious

Crypto Wallets 101

Basic Security

Disclaimer:

Here we present the bare minimum knowledge you need to make informed decisions while navigating decentralized applications.
However…

- **The crypto space is very new and there is no such thing as "completely safe" transaction.**
- **You can (and should) mitigate your risk by taking preventive security measures.**
- **Please, don't take my word for it, DYOR**

- **REMEMBER: If you want to participate of the decentralized ecosystem, keeping your assets secure is YOUR responsibility.**

What dangers are out there?

Bad Actors

People who want to steal from you

- **Hackers**
  - Find vulnerabilities in the code
- **Scammers**
  - phishing schemes

You

if you don't know what you're doing

- **Losing your keys**
  - Seed Phrase
  - Ledger
- **Making a mistake**
  - sending funds to the wrong network/address

What dangers are out there?

Bad Actors

People who want to steal from you

- **Hackers**
  - Keep your devices' OS up-to date
  - Use an encrypted email address
  - Always verify the website address you connect your wallet to.
  - Only follow links from trustworthy sources.
  - Diversify, diversify, diversify

- **Scammers**
  - NEVER click on any links shared by strangers
  - NEVER type your private keys anywhere, unless you are trying to restore your wallet.
  - Always verify information with a trusted source.
  - If something seems too good to be true, it probably is.

What dangers are out there?

You

if you don't know what you're doing

- **Losing your keys**
  - Lock your private keys in a secure place

- **Making a mistake**
  - Test before sending
  - Always double check
  - Don't transact while in a hurry

CryptoCurious

Conclusion

Conclusion

Do's

- Use an encrypted email address
  - Protonmail
- Use 2 Factor Authentication
  - Google Authenticator
- Use a hardware wallet as soon as you can get one
- Verify that DApps web addresses are accurate BEFORE connecting your wallet.

Don'ts

- Share your private keys
- Click unknown links
- Leave your crypto in exchanges
- Type your private keys anywhere
- DON'T TRUST. VERIFY

Thank you

Shirley McPhaul-Castro

shirley@prblockchain.org

@CrypticValky

Coming soon!

@CryptoCuriousPR