Crypto Wallet Hardening

Presentation by Carter and Christian Hinkle

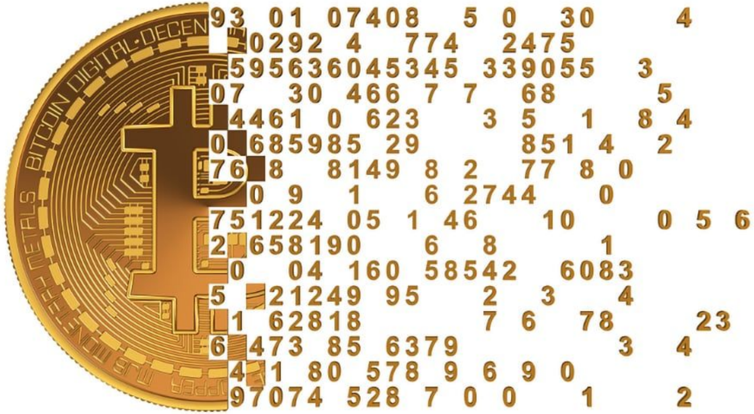
https://ekoios.vn/wp-content/uploads/2021/08/body-cryptowallet-secure.jpg

Let’s discuss what we will be working with

What is cryptocurrency

Cryptocurrency is currency that exists digitally and utilizes cryptography to verify its transactions.

- No such thing as physical coins for crypto (hence the “digitally”)
- Cryptography is crucial
- Assumed to be **decentralized** (peer-to-peer)

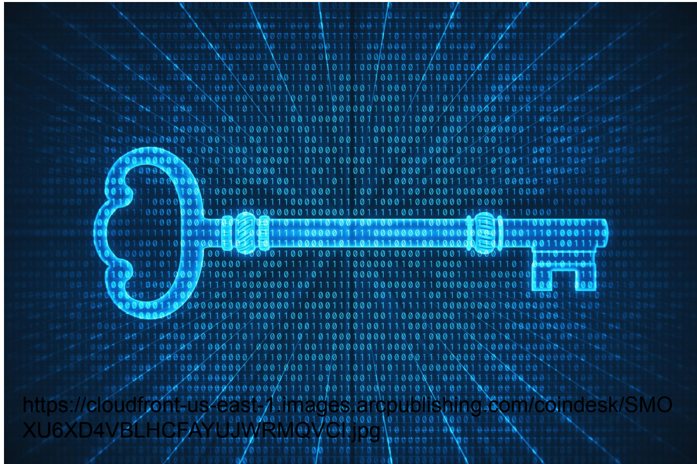


https://www.internettips.com/media/posts/264/bigstock-bitcoin-falling-apart-to-digital-bits-103147649-885x650.jpg

How do you get a wallet

Crypto wallets are claimed via **cryptography**

- Choose a private key (randomly generated and then recorded by the owner)
- This private key determines your wallet’s public key
- This private key is your way to provide signatures to your transactions
- Ownership of this private key means ownership of the wallet

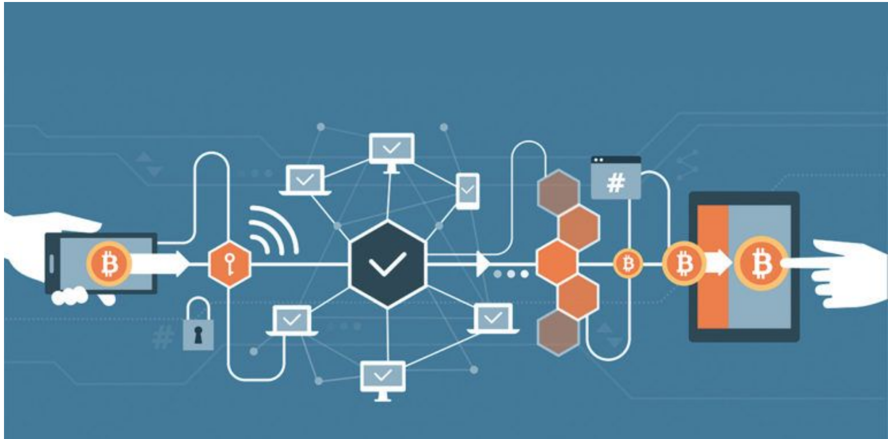


https://cloudfront-us-east-1.images.arcpublishing.com/coindesk/SMOXU6XD4VBLHCFAYUJWRMQVCI.jpg

How do transactions happen

Crypto transactions are processed using cryptography

- You make a transaction to another wallet (to their public key)
- This requires a **digital signature** from your wallet (derived from your private key)



https://s4769.pcdn.co/wp-content/uploads/2018/05/Cryptocurrency-Transactions-768x448.jpg

Where is the transaction history kept

The currency’s transaction history is what determines your wallet’s current balance.

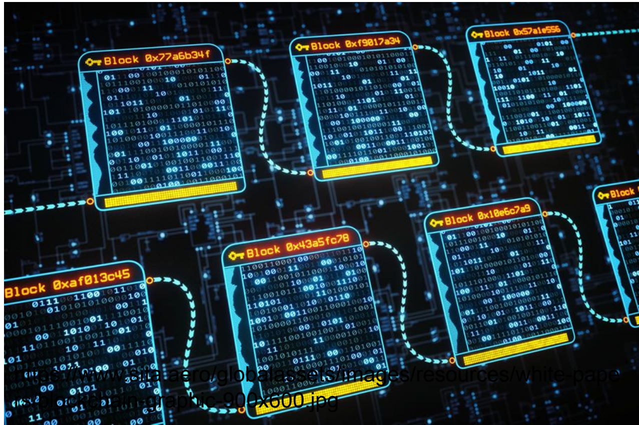
So where should it be kept? - This is what determines the decentralization of a cryptocurrency.

Centralized cryptocurrencies (BAD):

- Store transaction history on the company’s/government’s servers

Decentralized cryptocurrencies (GOOD):

- The history of transactions is agreed upon by the network
- This agreement method is called a **consensus mechanism**
    - Proof-of-Work (crypto mining)
    - Proof-of-Stake



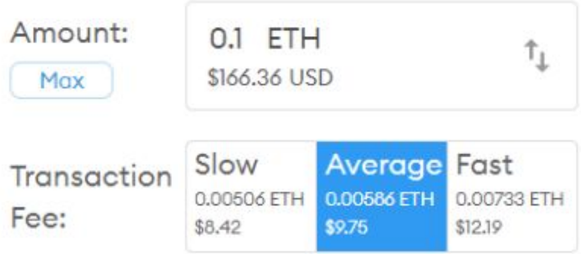
https://www.sita.aero/globalassets/images/resources/white-papers/blockchain-graphic-900x600.jpg

What is crypto mining?

The **Proof-of-Work** consensus mechanism

- Needed for the network of users to agree on transaction history (the blockchain)
- Puts transaction history in the hands of the network of miners
    - Rather than keeping transaction history on a centralized server

https://s.yimg.com/os/creatr-uploaded-images/2021-07/cae4bd60-ea00-11eb-b87f-5afc9ec8d43f



Amount: 0.1 ETH
$166.36 USD

Transaction Fee:

Slow	Average	Fast
0.00506 ETH	0.00586 ETH	0.00733 ETH
$8.42	$9.75	$12.19

Crypto wallet best practices

Avoid hosted wallet services

Hosted wallet examples:

- Coinbase
- Crypto.com
- Binance

These companies provide access to crypto wallets via their user accounts

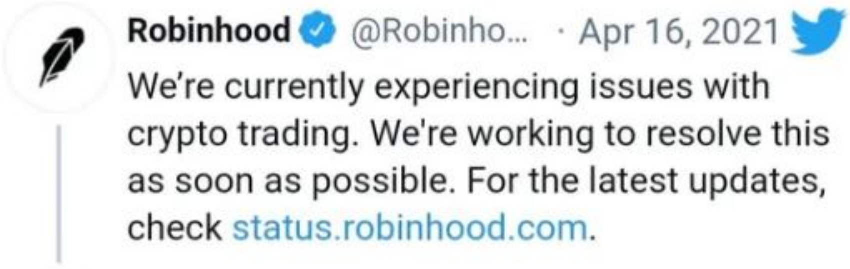
- They hold the private keys to your wallet
- You do not have access to your private keys
- They have the ability to lock you out of your wallet
- Hosted wallets are not your wallets - **not your keys, not your crypto!**

Only use these services for the purpose exchanging crypto and fiat currencies!

Avoid investing services

Example: Robinhood

- Lets you deposit and withdraw fiat
- Lets you exchange for crypto
- Does not give you an actual crypto wallet
- No private keys nor public keys!
- Cannot send crypto
- Focuses people’s attention on investment rather than usage



Robinhood @Robinho... · Apr 16, 2021

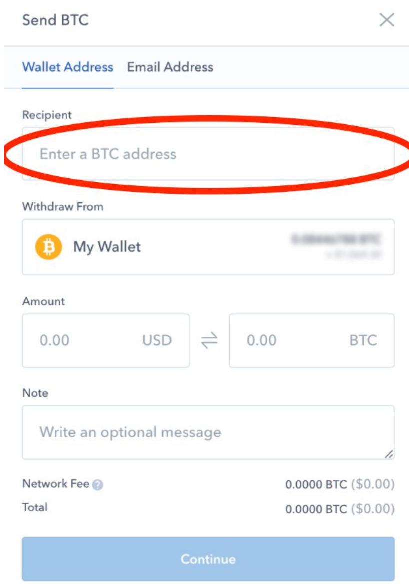
We’re currently experiencing issues with crypto trading. We're working to resolve this as soon as possible. For the latest updates, check status.robinhood.com.

If you choose a hosted wallet,

Services such as Coinbase, crypto.com, and Binance are much better options because they let you send your crypto wherever you like.

This can be used to purchase crypto, then send it to a cold wallet

For best practices, **do not use hosted wallets as a solution for long term crypto storage.**



Send BTC

Wallet Address Email Address

Recipient

Enter a BTC address

Withdraw From

My Wallet [redacted]

Amount

0.00 USD ⇌ 0.00 BTC

Note

Write an optional message

Network Fee 0.0000 BTC ($0.00)

Total 0.0000 BTC ($0.00)

Continue

Hot wallets and cold wallets

A **hot wallet** is a wallet on a device that is connected to the open internet

- Commonly open on a personal computer or mobile device
- Private keys are kept by the user

https://www.interactivecrypto.com/img/posts/13746.png

A **cold wallet** is a wallet on a device with limited internet connectivity

- Known as hardware wallets
- Private keys do not exist outside of the hardware device

https://cdn02.blockfer.com/images/wallets/best-3-hardware-wallets.png

Hot wallets versus Cold wallets

Pros:

- Convenient
- Integrates with personal devices
- Lets you view your private keys

Cons:

- Reliant on **software security**
- Reliant on physical security of your private keys

Pros:

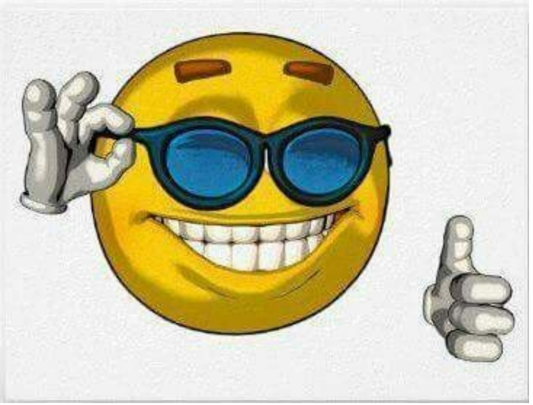
- Software security is irrelevant
- No concern of online attackers
- Your private keys do not exist outside of the hardware device

Cons:

- Reliant on **physical security**
- Concern of physical attackers
- Could misplace the wallet
- Could accidentally break the wallet

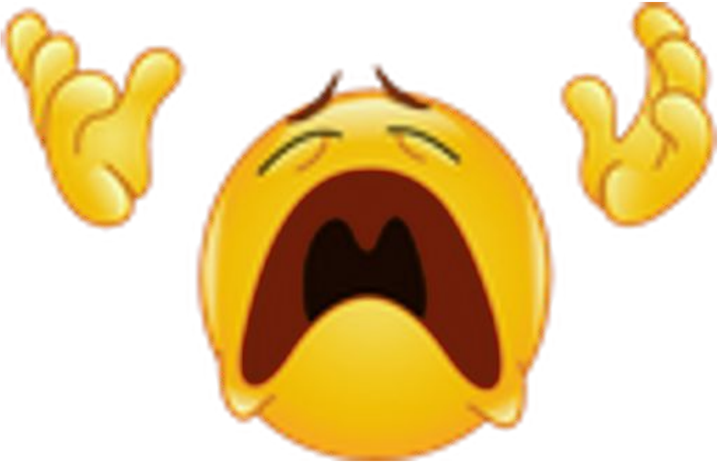
Crypto benefits

- Decentralizes currency
- Allows for a “backup” plan in case of inflation
- Convenient payment methods
- Puts you in control over your money



Crypto problems

- Energy cost
- Potential environmental footprint
- Potential centralization (miners or stakers all part of same region)
- Secure options are unintuitive
- Money can easily be lost (typing in a public key incorrectly)
- Hype trains
- Currently made up of many scammers



Let’s secure a crypto wallet!

Assignment general instructions

- Download Exodus wallet
- Download and install WinRAR
- Backup your private key **seed phrase**
- Download your seed phrase to your local disk
- Create an encrypted archive of your seed phrase and password via WinRAR
- Remember this password to access your private keys
- Delete the unencrypted seed phrase files

https://topcryptonewss.com/wp-content/uploads/2021/07/maxresdefault-8.jpg