Cryptocurrency:

Wallet Creation & Protection

Kayla Dixon & Andrew Burbage

What is it?

- Cryptocurrency is is a digital currency and alternative form of payment
- Decentralized Finance
- Made using encryption algorithms
- Can be purchased or “mined”

Image Source: pngtree.com/so/ethereum-bitcoin

Is Cryptocurrency Money?

- Yes, technically...
  - While it does hold monetary value it acts almost like a stock or investment
  - Unlike currency or credit from a bank there is no backing by the US government like the FDIC
  - Lack of backing or regulation makes it unstable but appealing to some

How does it work?

- As mentioned before it is either bought or “mined”
  - Buying is quite similar to buying a stock in the modern age where there are various apps and services that allow for a broker like exchange or real money for crypto at market value
  - However, crypto can be “mined” where new coins are created through validating transactions of existing coin in the chain
  - Hard Forking is another alternative method

Crypto Wallets

- There are 3 types of wallets used to store cryptocurrency
  - Hardware
  - Paper
  - Software
- Hardware and Paper wallets are considered “cold” while software is considered “hot”
- All wallets are designed to store the public and private keys used for ownership and transfer of cryptocurrency

Hardware Wallets

- Hardware wallets are a physical device
- Offer increased security compared to software wallets
- Popular models include the Ledger Nano S and Trezor

Image Source:fempreneur.space/hardware-wallets-tested-ledger-vs-trezor-more-security-for-your-cryptocurrencies

Paper Wallets

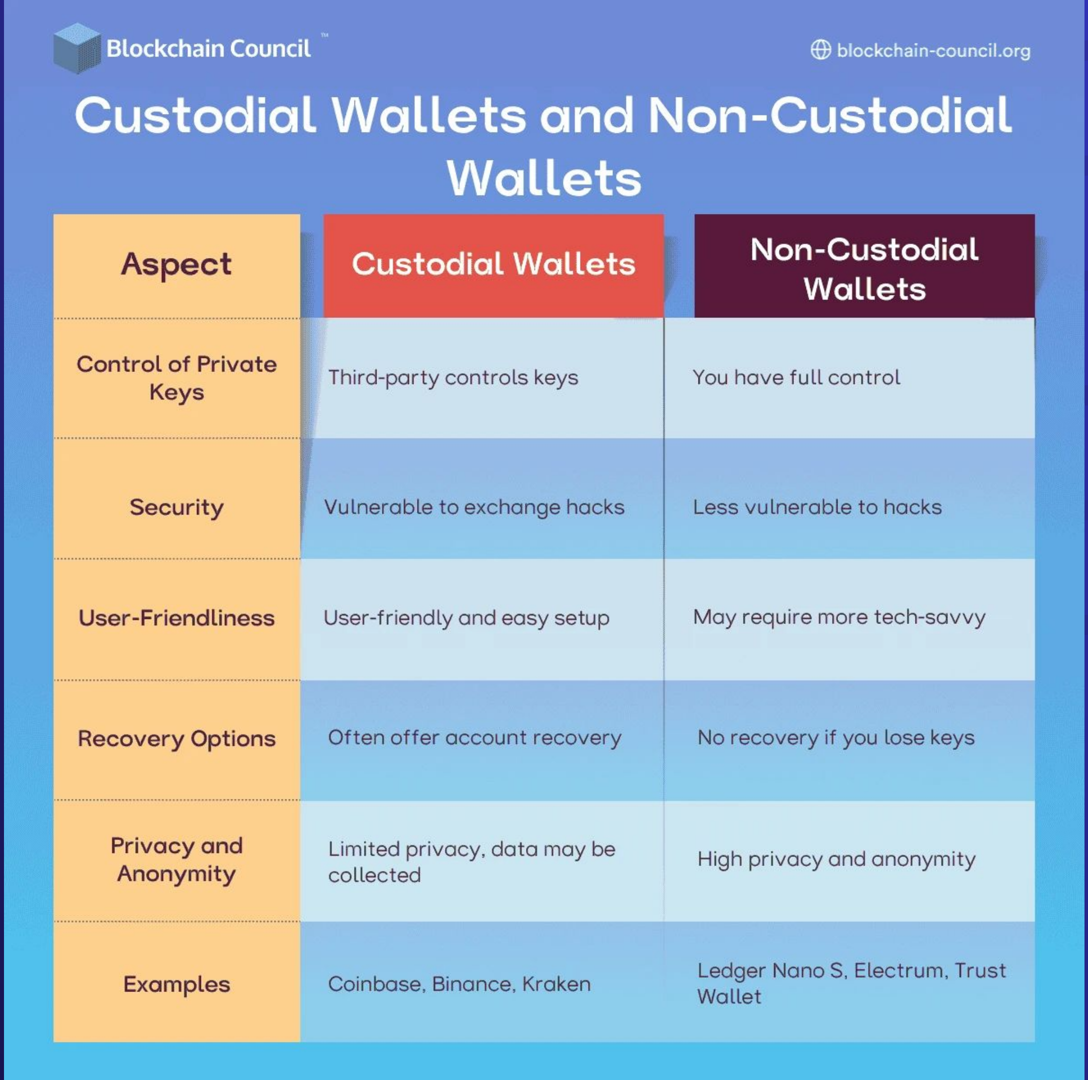
- As the name suggests these are wallets where the keys are stored strictly on paper
- These are considered the most secure option
- However they are often looked at as obsolete due to the difficulty of transfer

Image Source: thewolfofallstreets.io/how-to-create-your-first-bitcoin-wallet/

Software Wallets

- Can be desktop, mobile, or web based
- Desktop is the most secure of these three but requires extra protection due to connection to the internet(Coin Wallet, Bitcoin Core, and Electrum)
- Mobile is are similar in safety and are appealing due to the ease of access but vulnerable as well (Coinomi and Mycelium)
- Web based is considered very vulnerable and are usually only used for small transactions (MetaMask and Coinbase)

One More Distinction



Blockchain Council™

blockchain-council.org

Custodial Wallets and Non-Custodial Wallets

Aspect	Custodial Wallets	Non-Custodial Wallets
Control of Private Keys	Third-party controls keys	You have full control
Security	Vulnerable to exchange hacks	Less vulnerable to hacks
User-Friendliness	User-friendly and easy setup	May require more tech-savvy
Recovery Options	Often offer account recovery	No recovery if you lose keys
Privacy and Anonymity	Limited privacy, data may be collected	High privacy and anonymity
Examples	Coinbase, Binance, Kraken	Ledger Nano S, Electrum, Trust Wallet

Why Teach Crypto Wallet Security in Cyber Security?

- As Cryptocurrency has become more prevalent in society we have seen it spread beyond private individuals into various industries and even major companies
- There will continue to be an increase in a need for professionals who can identify and mitigate risks to prevent attacks and theft
- Some even argue that it could possibly replace our current currency based financial structure

Current risks and threats

Phishing:

- Dominic Lacovone had $650,000 in crypto siphoned from his wallet after perpetrators posed as apple support to gain access to his iCloud where his MetaMask recovery phase was stored.

Hacking:

- During the Lastpass incident over $4.4 million was stolen after vulnerabilities on 80-85 distinct wallets were taken advantage of

Private Key Theft:

- Slope Wallet retained users' private keys in their logs leading to $4 million in theft

Exchange Vulnerabilities and Malware:

- Like above vulnerabilities can be found, or amplified by malware, & used to steal from users

Mitigations Available

There are a few obvious options:

- Use strong unique passwords
- Enable Two-Factor Authentication (Like Google or Microsoft Authenticator)
- Be vigilant against Phishing attacks
- Store bulk of currency in "Cold" wallets
- Monitor Accounts Regularly

More Advanced Options

- Stay up to date on best software for security
- Consider using a VPN
- Secure Backup Keys and Seed Phrases

QUESTIONS?

Resources

Federal Trade Commission

https://consumer.ftc.gov/node/77130

Coursera

https://www.coursera.org/articles/how-does-cryptocurrency-work

Blockchain Council

https://www.blockchain-council.org/blockchain/types-of-crypto-wallets-explained/

https://www.blockchain-council.org/cryptocurrency/crypto-security-tips/