



# Bitcoin Wallets

**Nevada County Bitcoin Meetup**  
**September 21, 2022**

# Obligatory Disclosures

This is for educational and entertainment purposes only.

This is not investment advice.

We are not financial advisers.

Do your own research prior to purchasing ANY financial instruments.

We DO NOT advocate you purchase bitcoin.

We are here as a resource.

Ultimately, you must decide what is best for yourself.

We will not allow discussion of other cryptocurrencies; Make your own group.

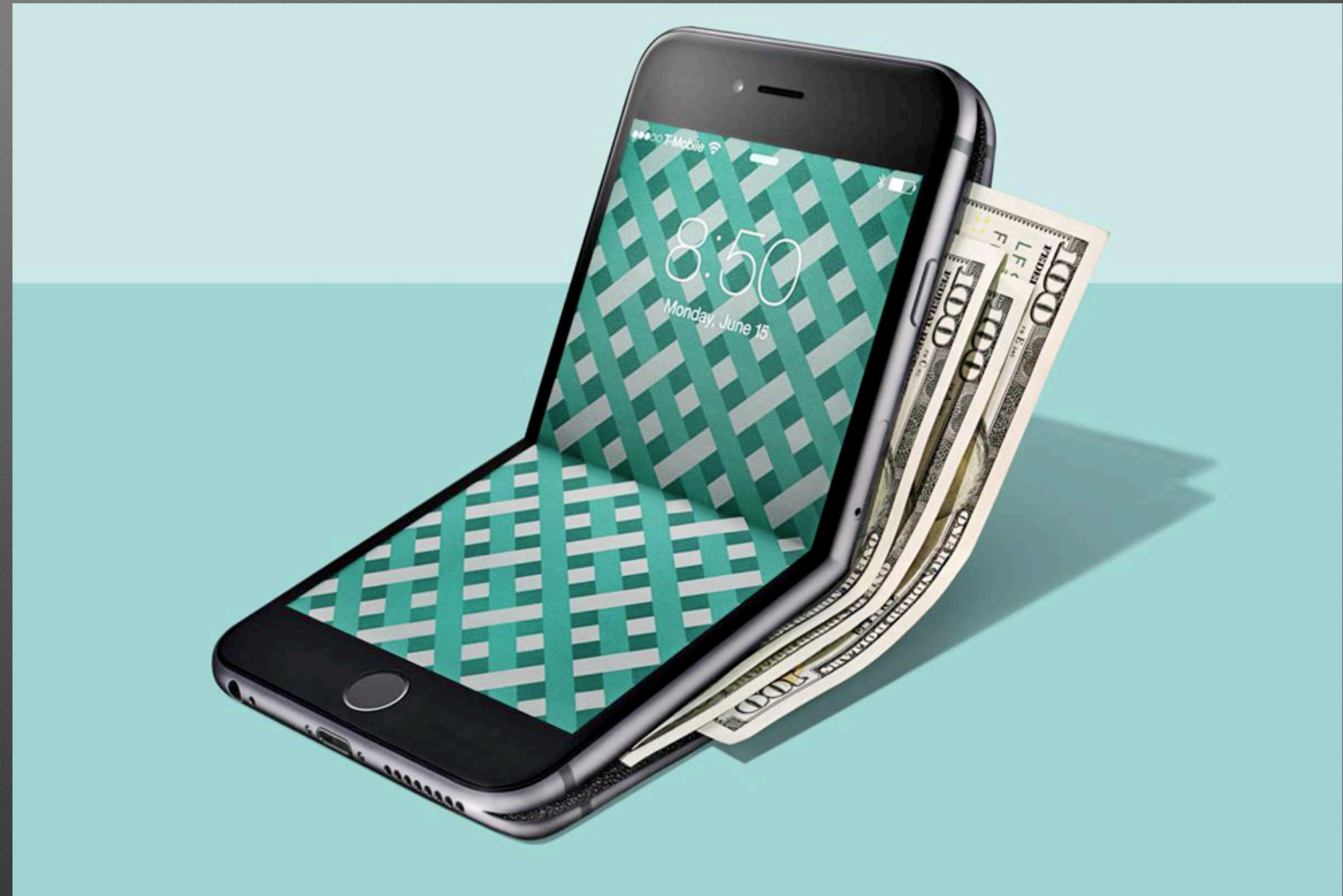


**Any current event questions?**

**General questions welcomed, also!**

# Review: Wallets

- Wallets are software for your computer or phone
- Wallets allow bitcoin to be received and spent
- Most of the technical aspects of the wallet are done behind the scenes
- Wallets can be open or closed source



# How Do Bitcoin Wallets Work? (cont'd)



- What is a private/public key pair?
- Key pairs are generated together through cryptography and are mathematically related
- This is often completed by the wallet software with minimal involvement by user
- Public key is viewable on the blockchain
- Private key is only known by the owner of the key pair
- Private key allows owner prove ownership of public key (e.g., create, sign, and transmit a bitcoin transaction)

<b>Bitcoin Address</b>		<b>Private Key</b>
	<b>SHARE</b>	
1ByqLdKS7vSgvNhFXzrLQ6GBcygNp3rpQn	<b>SECRET</b>	L2UqgVvE75oS9C7Kkci7FmXgXXpsNvtU83FkN7EG2WTPzUEPfmBu

Real key pair generated at [bitaddress.com](https://bitaddress.com)

# Review: Transactions

## Transaction

d2189650915eb83bd3bc421490d089f71352c7198b6459c879aecf4e5e3da4d4

Unconfirmed

First seen *Just now*

Fee 3,456 sat **\$0.84**

ETA In ~10 minutes

Fee rate 31.6 sat/vB

Features **SegWit** **Taproot** **RBF**

## Inputs & Outputs

Details

bc1qpgp4wzaya5uk405n77satdkwj.gwr3sq8jmg

0.00280182 BTC

bc1q0956d0619vgpz47tj3rww0ahu.r9uc690tqy

0.00276726 BTC

0.00276726 BTC

## Details

Size 191 B

Version 1

Virtual size 109.25 vB

Locktime 0

Weight 437 wU

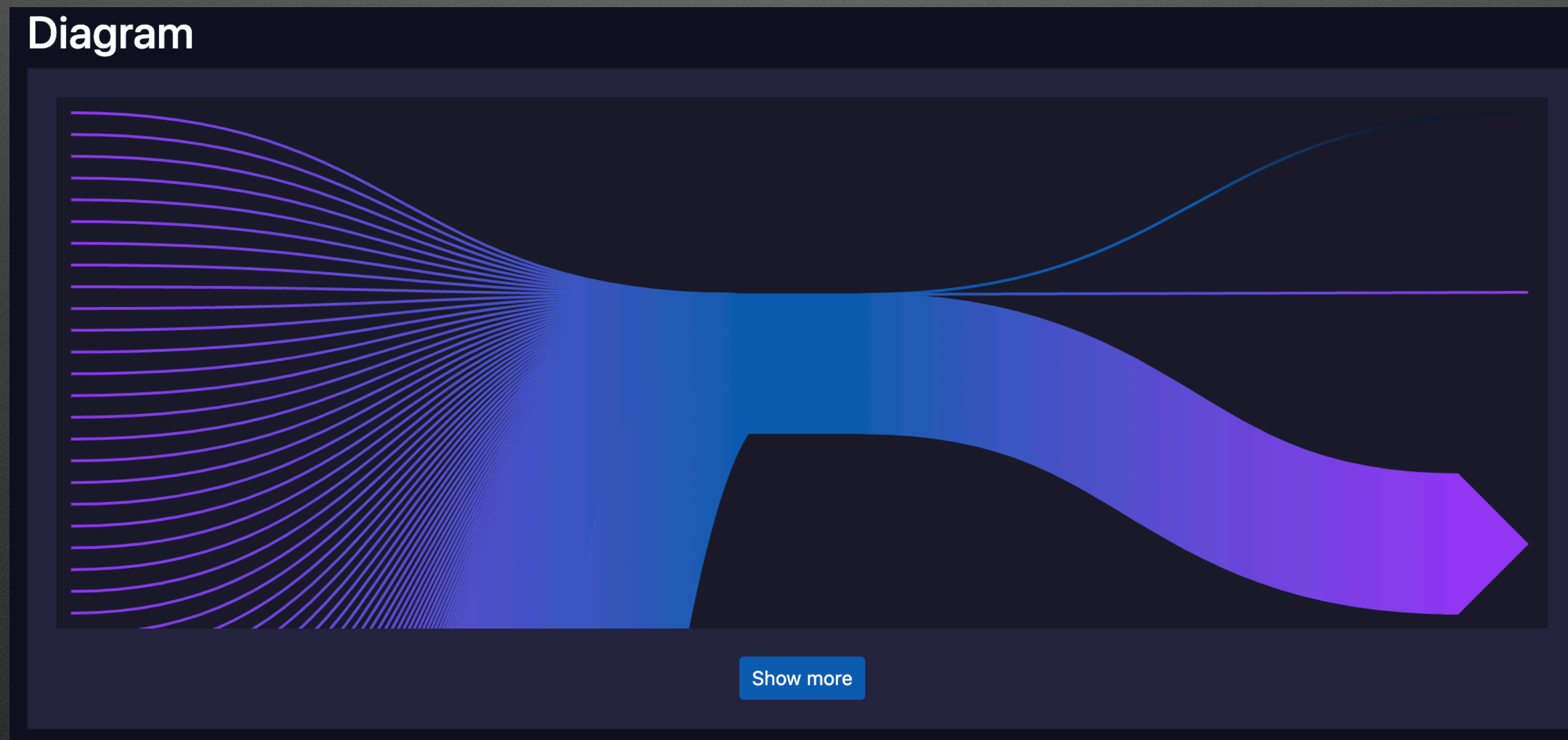
Transaction hex [↗](#)

- A “transaction” refers to a transfer of bitcoin from one address to another.
- Each transaction has a “transaction ID” that can be used to look up the transaction details
- A blockchain explorer is a website that can show transaction details by querying the bitcoin blockchain

# But what does a wallet really do?

Aggregates transactions and coordinates sends through an easy interface

## Mempool Transaction



# Review:

## Open Source vs Closed Source

Open source software is software with source code that anyone can inspect, modify, and enhance.

- Examples of Open Source Wallets:
  - BlueWallet
  - Muun
  - Cake Wallet
  - Phoenix

Closed source software has source code that only the person, team, or organization who created it—and maintains exclusive control over it—can modify.

- Examples of Closed Source Wallets:
  - Strike!
  - Cash App
  - Coinbase
  - Exodus



# Wallet Recommendations



**Muun**

Self Custodial  
Lightning and  
On-Chain



**BlueWallet**

Self Custodial  
Lightning and  
On-Chain



**Wallet of Satoshi**

Custodial  
Lightning Only

# Why is Open Source Important?

- Accessible to everyone
- Auditable
- Malleable
  - Don't like it? Change it.
- Inter-operable
- International

## BITNODES

Bitnodes estimates the relative size of the Bitcoin peer-to-peer network by finding all of its reachable nodes.

### REACHABLE BITCOIN NODES

Updated: Mon Sep 19 09:21:11 2022 PDT

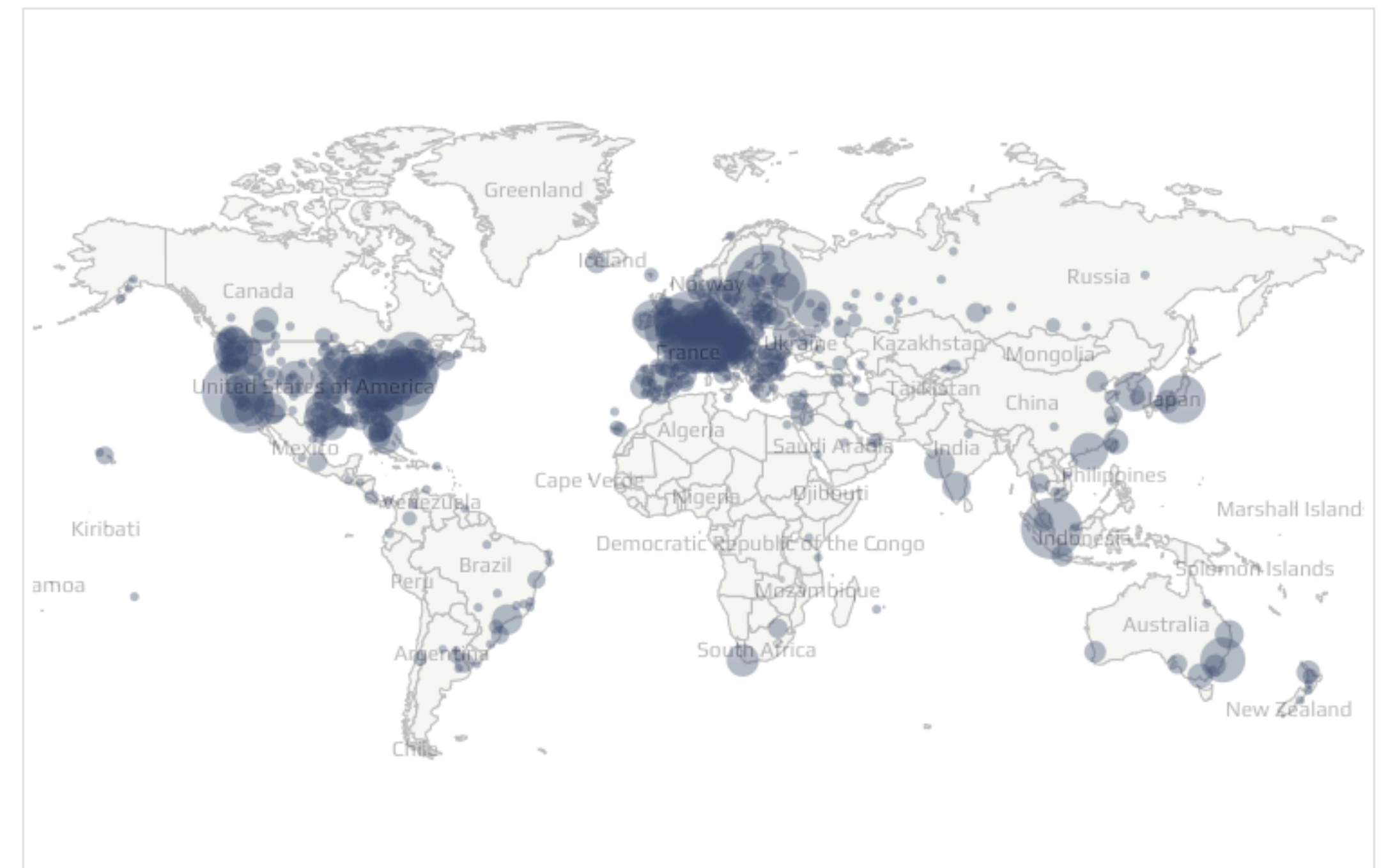
14143 NODES

CHARTS

Top 10 countries with their respective number of reachable nodes are as follow.

RANK	COUNTRY	NODES
1	n/a	7051 (49.86%)
2	United States	1961 (13.87%)
3	Germany	1413 (9.99%)
4	France	448 (3.17%)
5	Netherlands	384 (2.72%)
6	Canada	319 (2.26%)
7	Finland	248 (1.75%)
8	United Kingdom	217 (1.53%)
9	Russian Federation	182 (1.29%)
10	Singapore	145 (1.03%)

All (96) »



Map shows concentration of reachable Bitcoin nodes found in countries around the world.

LIVE MAP

# Company/Custodial Wallets

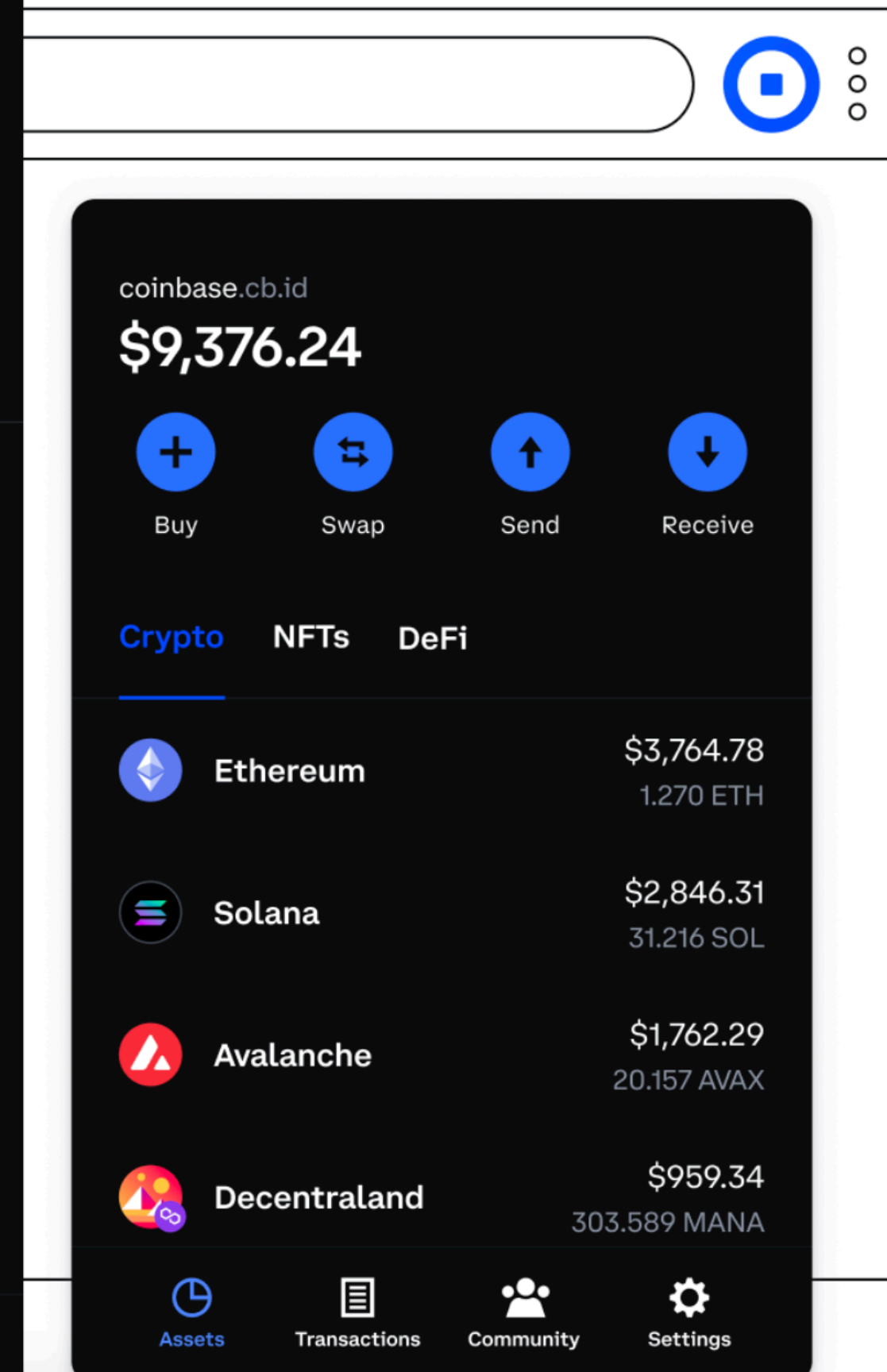
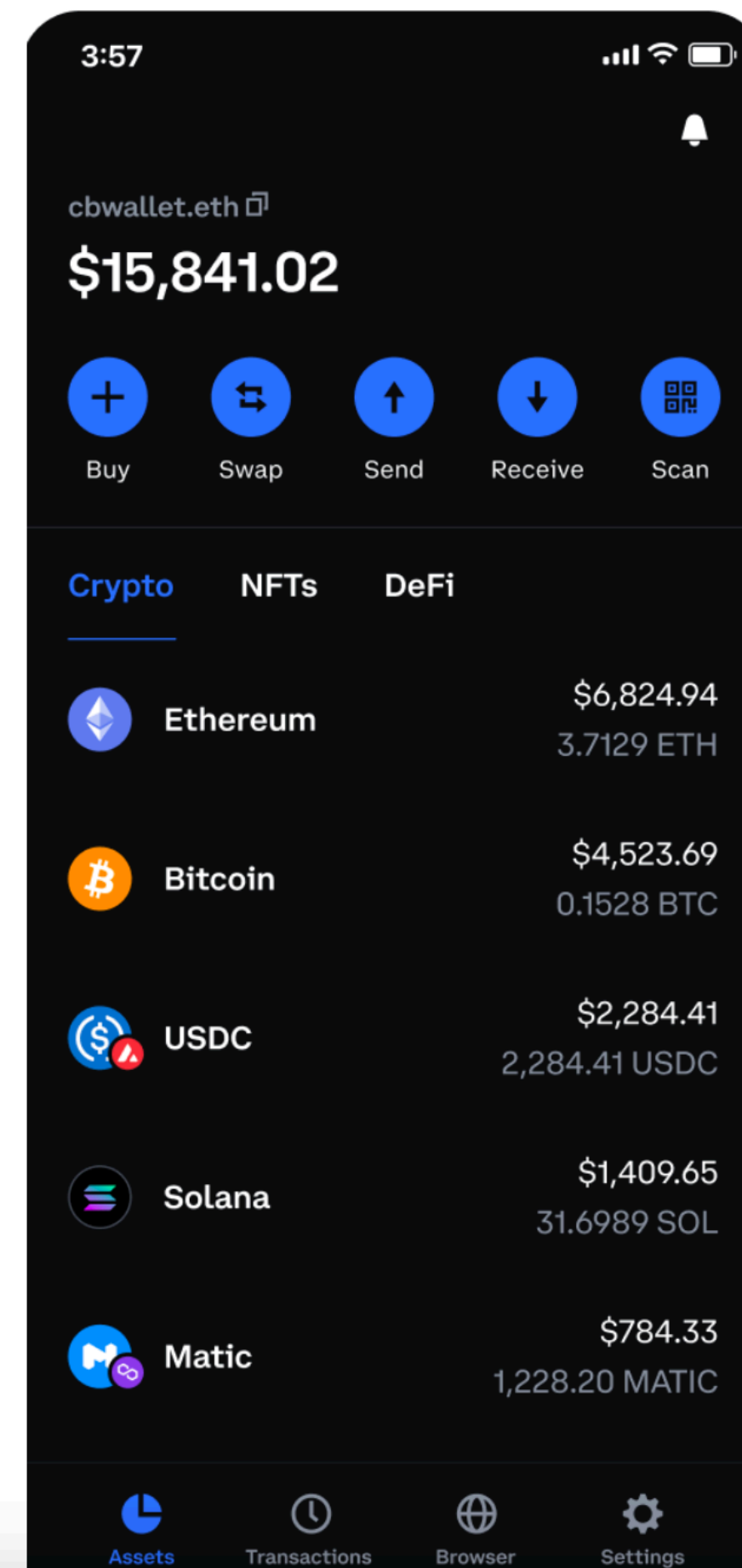
WALLET

## Coinbase Wallet

Your key to the world of crypto

- Store all of your crypto and NFTs in one place
- Support for hundreds of thousands of tokens and a whole world of dapps
- Explore the decentralized web on your phone or browser
- Protect your digital assets with industry-leading security

Download Coinbase Wallet



# Concerns with Closed Source (Company) Wallets

- Some are not bitcoin only; business model promotes sh\*tcoin gambling
- Wants owners to connect to company service (to purchase crypto)
- \*Does not value privacy\*
  - Logs IP addresses
  - Logs Transactions
  - Targeted Marketing



# Why are Company/Custodial Beneficial?

- They do allow for purchase of bitcoin
  - Not all allow withdrawals, though
- If you are unable to withdraw your bitcoin, you CANNOT guarantee you \*own\* that bitcoin
  - You may just own a dollar claim on a percentage of bitcoin, which opens the door for other issues if you actually want the bitcoin
- Support/account recovery is possible and easy

# Excerpts from Coinbase Wallet

## Coinbase Wallet Privacy Policy

Last Updated: August 31, 2021

Coinbase Wallet (also known as Toshi Wallet) is a software service accessible via a mobile device application and a browser service for the Ethereum Network (the "Network") distributed by Toshi Holdings Pte. Ltd ("Toshi Holdings" or "we" or "us" or "our") that enables users to (i) self custody digital assets; (ii) access a digital asset browser and link to decentralized applications and decentralized exchanges; (iii) view addresses and information that are part of digital asset networks and broadcast transactions; and (iv) additional functionality as Toshi Holdings may add to the app from time to time (collectively, the "App" or "Coinbase Wallet"). This Privacy Policy ("Privacy Policy") helps explain how we collect, use, store, and protect your information when you use the App, our developer software, or our website at <https://wallet.coinbase.com/> (collectively the "Services"). Please also read [Coinbase Wallet's Terms of Service](#) (the "Terms"), which describe the terms under which you use the Services.

### Information We Collect

We receive or collect information when we operate and provide our Services, including when you install, access, or use our Services.

Information you provide

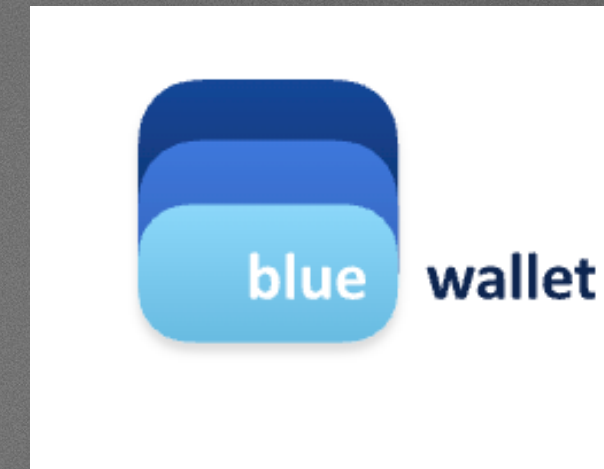
- **Your Account Information** - In order to create a Coinbase Wallet account, you will provide us with a username. You may also voluntarily add other information, such as a username.
- **Your Transactions** - Your Network private key, which you utilize to access your funds and initiate transactions, is stored only on your own device. However, to facilitate your transactions and provide you with your account balance, we store the Network public key address associated with your Network private key.
- **Customer Support** - We may collect additional information you may disclose to our customer support team.

# Continued Excerpts from Coinbase Wallet

## Automatically collected information

- **Metrics and Performance Data** - We may collect service-related, diagnostic, and performance information. This includes high level information about your activity (such as how you use our Services and how you interact with others using our Services), and diagnostic, crash, website, and performance logs and reports.
- **Device and Connection Information** - We may collect device-specific information when you install, access, or use our Services. This may include your IP address and, if you choose to allow push notifications through Coinbase Wallet, your device's unique push token. We may also temporarily collect information about decentralized applications (dapps) that you are connecting to, while establishing that connection.
- **Status Information** - We may collect information about your online status on our Services, such as when you last used our Services (your "last seen status").

# Compare to



The company's policy is to collect as little user information as possible to ensure a completely private and anonymous user experience when using the Service. We also have no technical means to access your encrypted storage content in any case.

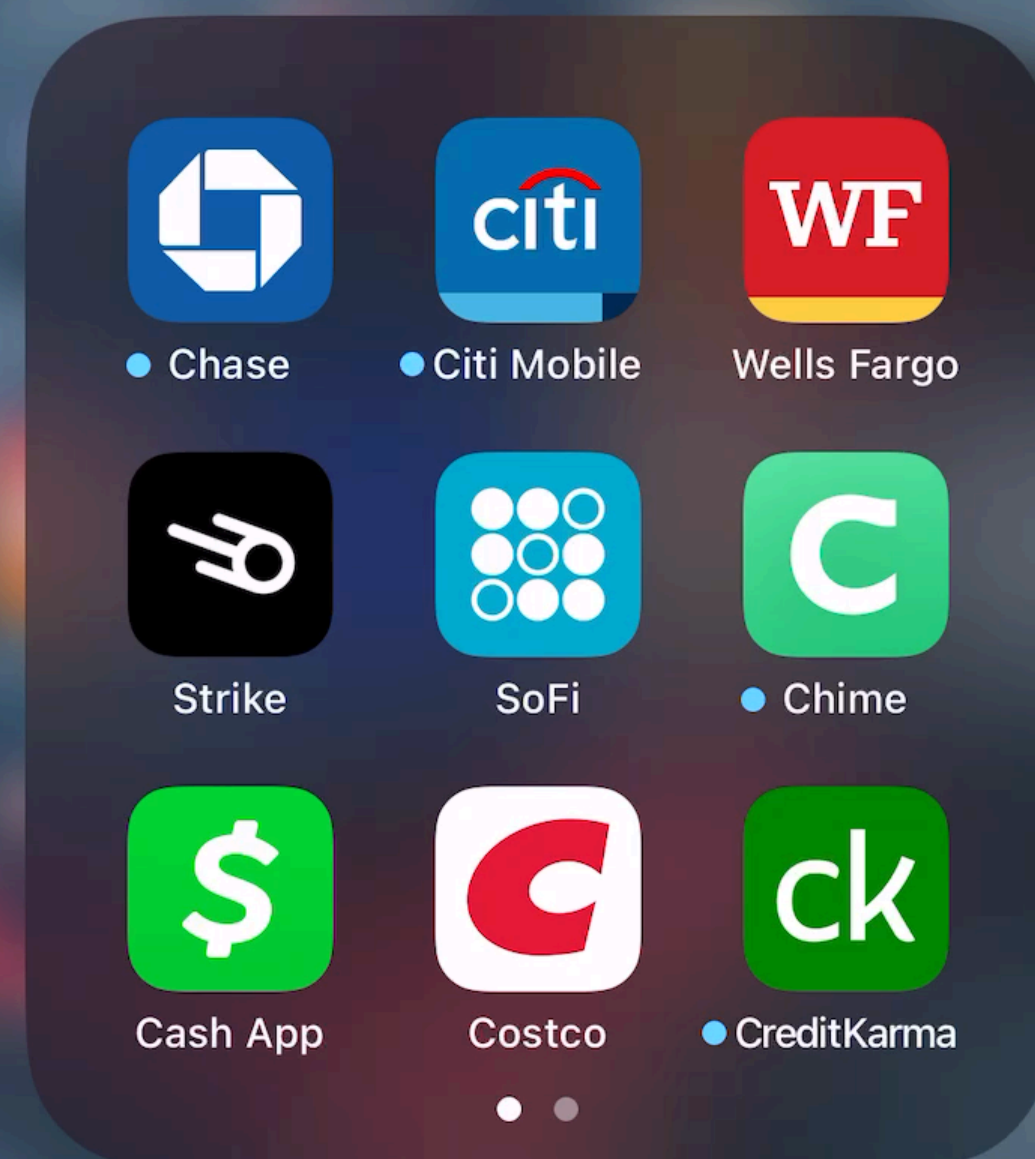
Aggregated data and basic usage events for analytics and application crashes are collected in order to maintain the integrity of the service and help users debug in case of errors. This data collection can be opt-out by the user at any moment from the application settings privacy options.



# Custodial

Banking

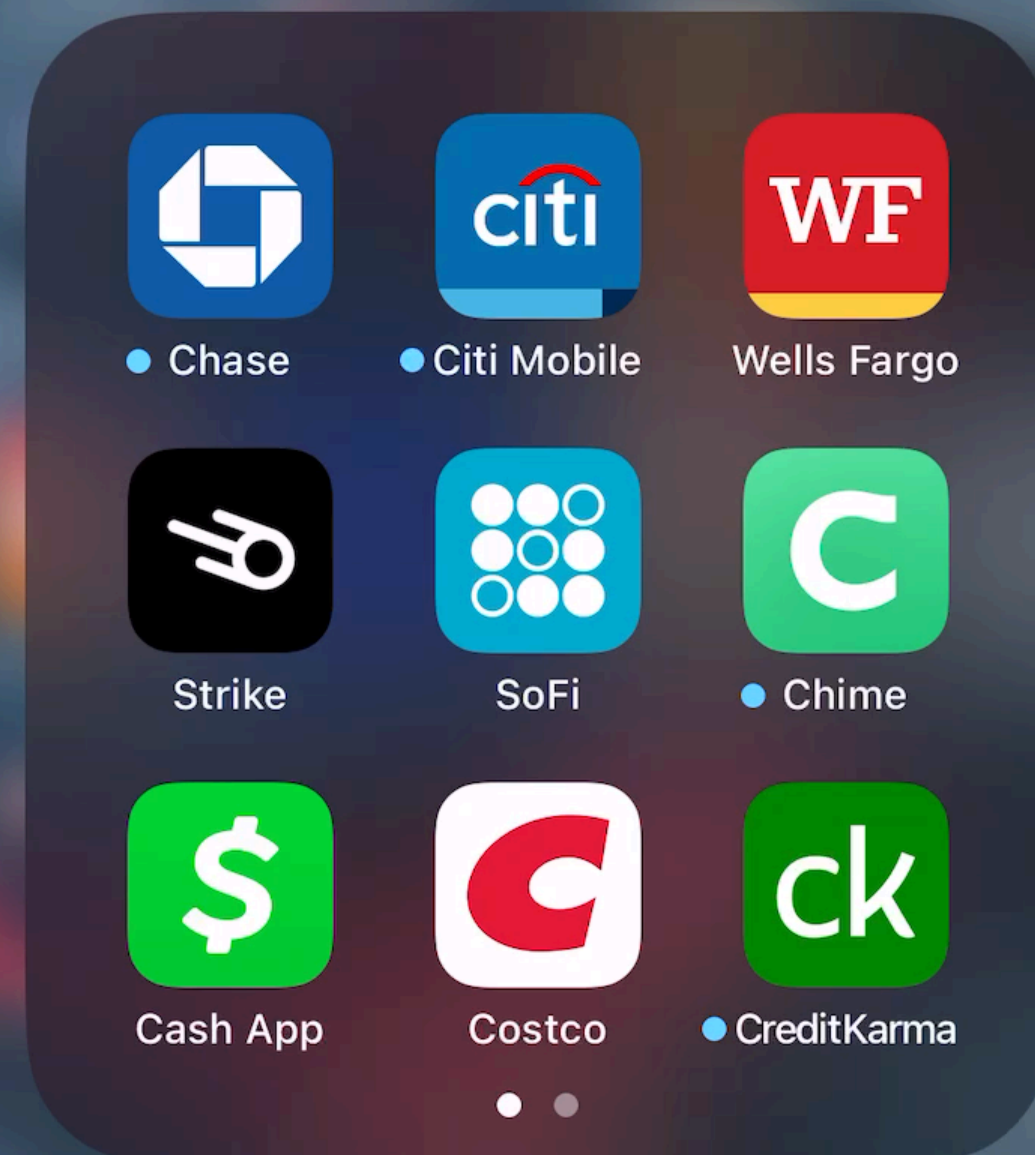
# -Throughs



# Custodial

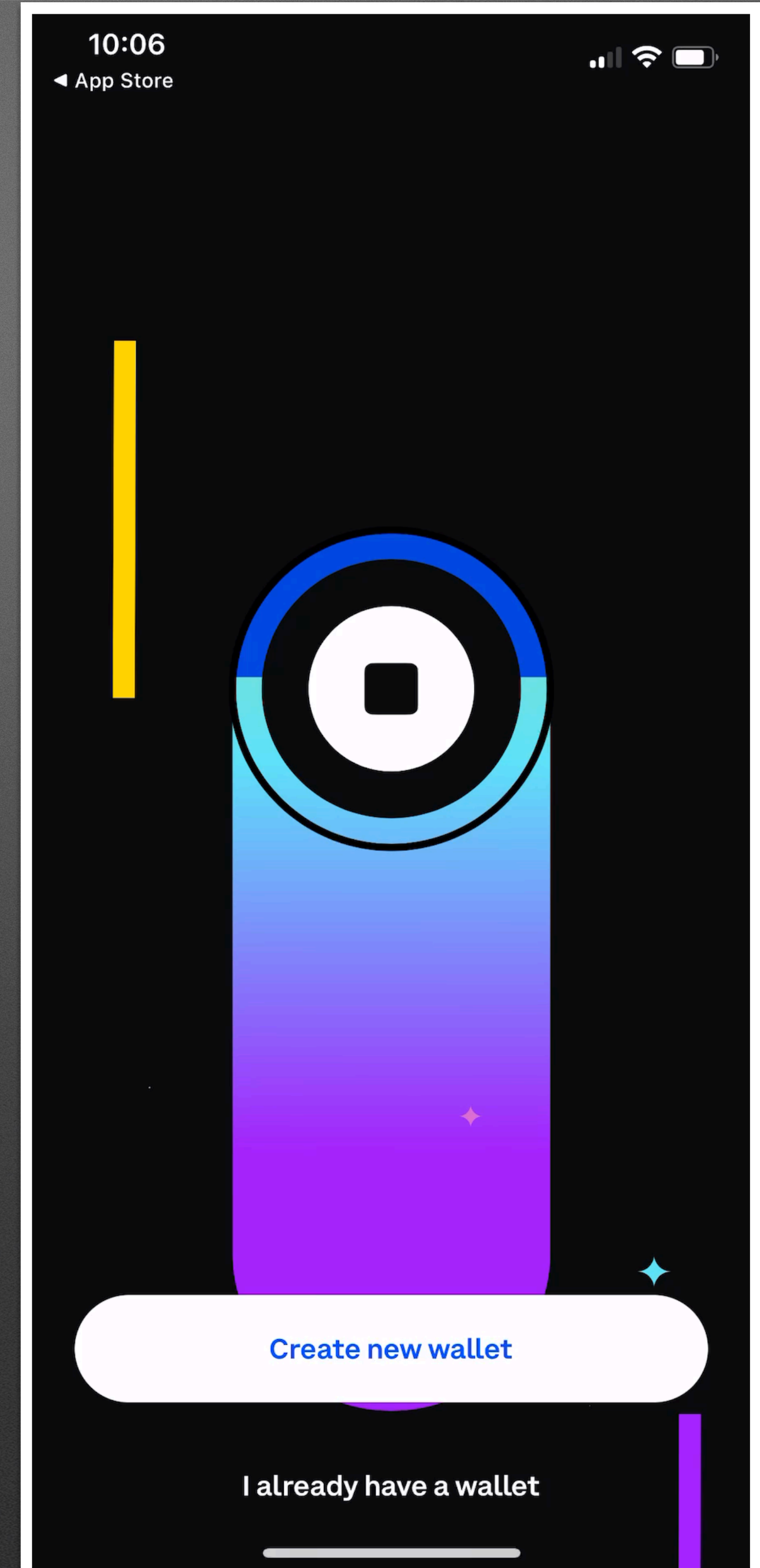
Banking

# -Throughs

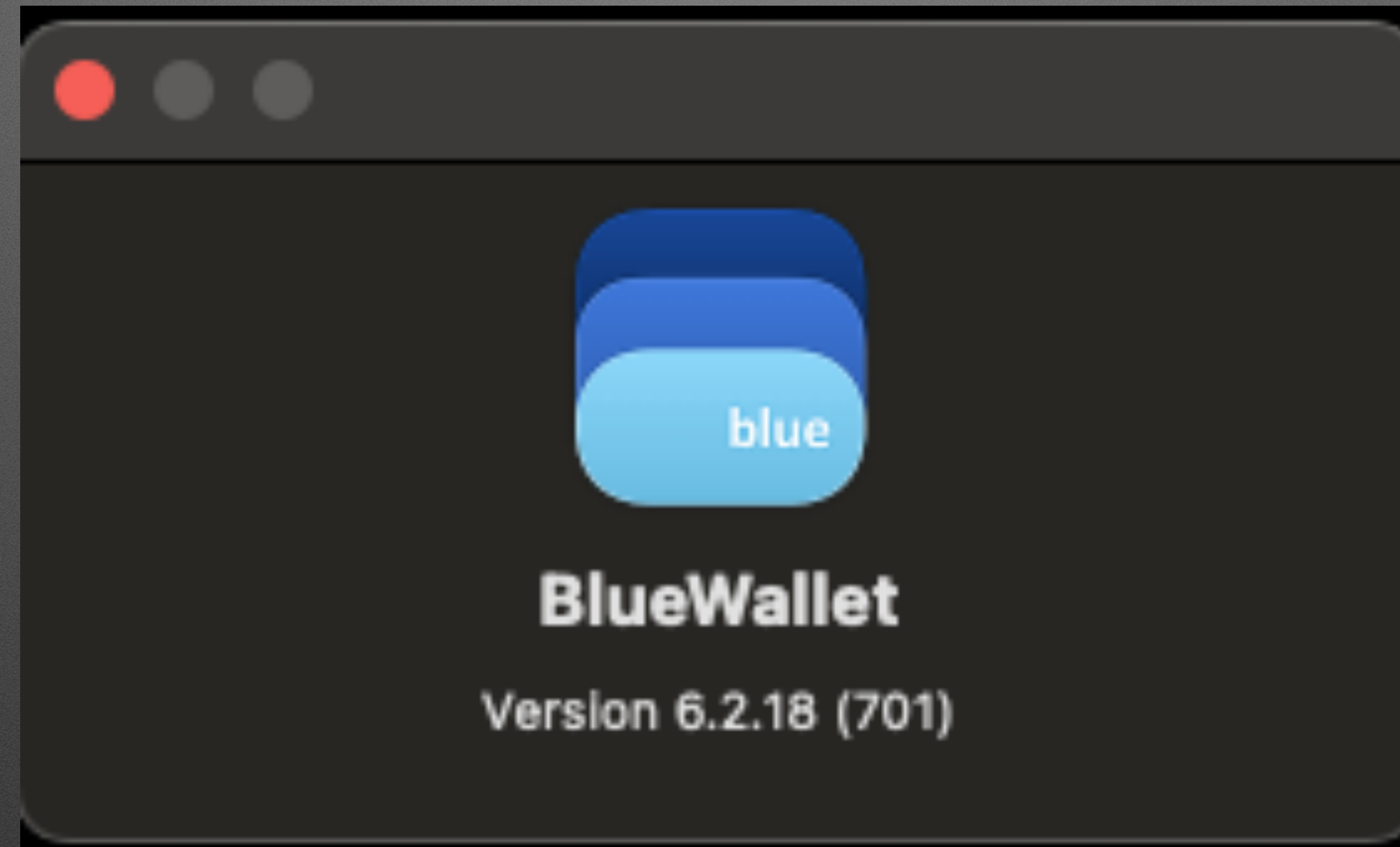


# Setting Up Wallets

## Coinbase

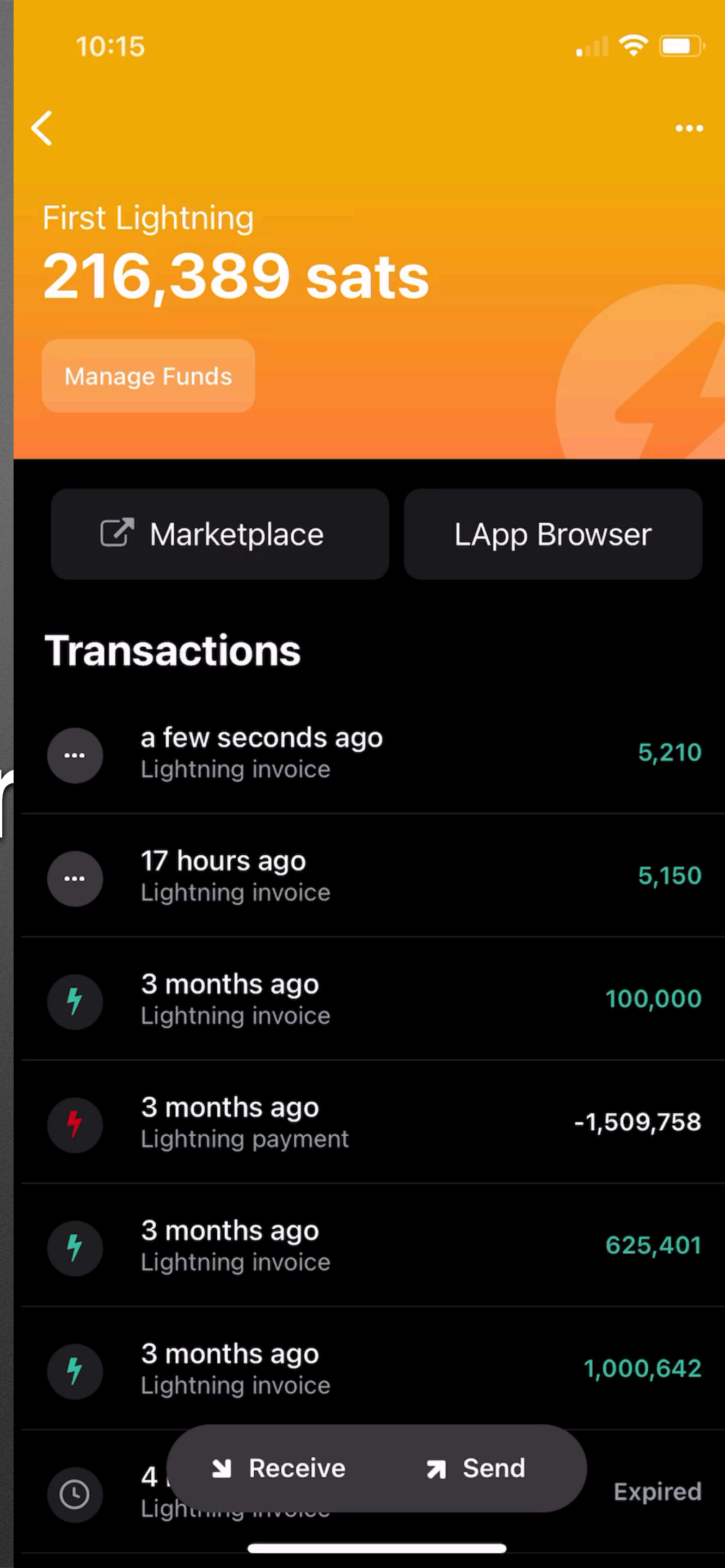


# Setting up and Funding Self-Custody Wallet with BlueWallet (Mac)



Quick Note: This is a topic that needs more time. You will see a security advisement to write down several words. This is a mnemonic phrase, which we will discuss next month.

What does it



ity look like?

# Live Transactions Demonstration


We will use Cash App, Strike,  
BlueWallet, Muun, and Wallet of  
Satoshi



# In Conclusion: Real-World Uses Matter



**Questions,  
Comments,  
Concerns,  
Suggestions?**



Any sufficiently advanced  
technology is  
indistinguishable from magic.

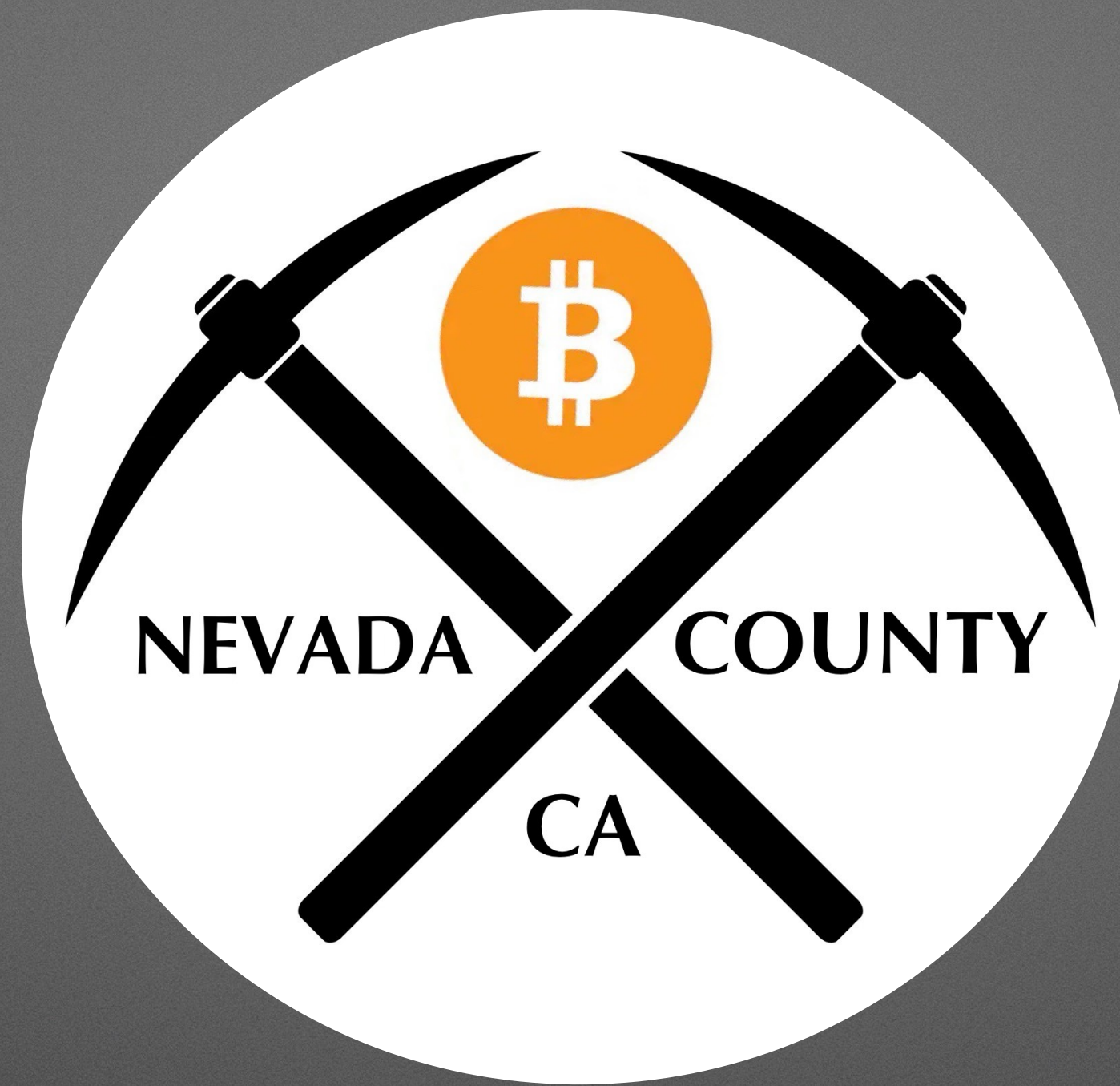
Arthur C. Clarke

quote fancy



# Exciting Announcement!

[Click here to find out more!](#)



**Thanks for Joining Us!**  
**Next Meeting: October 19, 2022**  
**Topic: Bitcoin Best Practices**