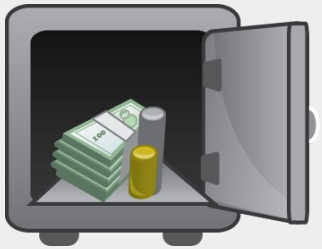
The Basics of Wallets & Wallet Security

A Little About Me...

- Software Engineer @ Microsoft in Pittsburgh
- Run https://chaintuts.com creating Bitcoin & blockchain related tutorials
  - Articles, videos, and code projects
  - On YouTube, Twitter, Github
  - Support: Patreon, Crypto, Spreadshirt Apparel
- Focus is on understanding & teaching core concepts

First, A Quick Disclaimer

- Security is a *complex, evolving* topic
- There is not a one size fits all solution
- Know your threat model, and learn about tools you can use
- **We'll discuss some Bitcoin fundamentals and the surrounding security tools**

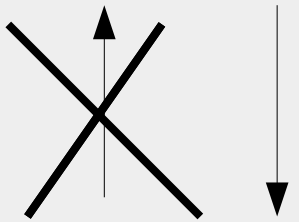


What Exactly is a Wallet?

- Really a collection of *private keys*
- Private keys used to be randomly generated, but now come from a *seed phrase*
- Crypto-secure seed encoded as words for easy backup

What Exactly is a Wallet?

0x12351bc143badf2348fe38e8f8b785b...

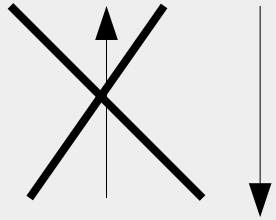


Elliptic Curve
(secp256k1)

PRIVATE KEY

0x04135981abcd7f7a7d7b7c720….

PUBLIC KEY



“Double hash” (SHA-256
and RIPEMD160)
And Base58check encoding

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

ADDRESS
(PUBLIC KEY
HASH)

What Exactly is a Wallet?

0x2352bca23aafd389… encoded as word1, word2

SEED PHRASE

Privkey child

Privkey child

PRIVATE KEYS

Privkey grandchild

Privkey grandchild

Privkey grandchild

Privkey grandchild

What Exactly is a Wallet?

- The process of deriving keys from a seed phrase is *deterministic*
- Same seed phrase, same keys, same addresses when restoring a wallet!
- With one caveat...

What Exactly is a Wallet?

- Different wallets use different *derivation paths*
- Ex: m/44’/0’/0’/0/0
  - M/44’ is constant
  - 0’ is Bitcoin
  - 0’ is the first *account*
  - 0 means external, 1 for change addrs
  - 0 is the first address

What Exactly is a Wallet?

- What about addresses, transactions, balances, etc.???
- All of that is stored on the public blockchain, NOT in the wallet!
- Wallet software simply fetches this data as needed, or stores the full chain

Private Keys & The #1 Rule...

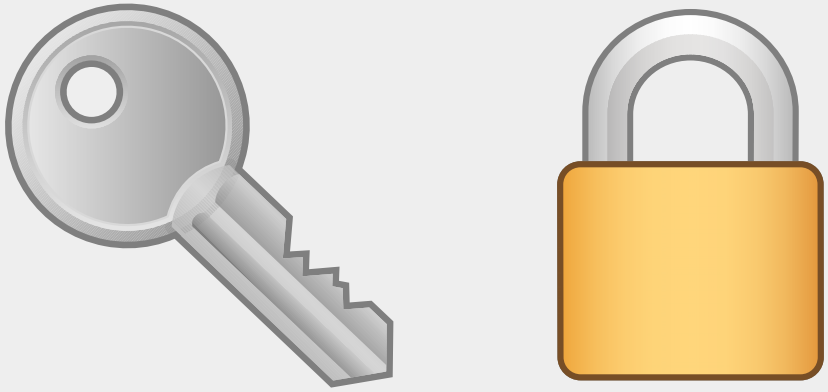
Not your keys…

NOT YOUR BITCOIN

Private Keys & The #2 Rule...

Not your keys…

NOT YOUR BITCOIN



Types of Wallets

- Custodial Wallets
- Online Wallets (SPV & Full Node)
- Offline Wallets (Hardware & Paper Wallets)

Custodial Wallets

- Ex: Coinbase, Binance, etc.
- Hold private keys for you, doesn’t give a seed phrase
- Pros: Ease of use, ease of security
  - Great if you’re new or less tech savvy
- Cons: Not your keys, not your coins!
  - Ultimately like a traditional bank model that can fail (Mt. Gox)

Online Wallets

- Ex: Coinomi, Bitcoin.com, Bitcoin Core
- Wallet is on an *online* device
- You control private keys (seed phrase)
- Pros: Still easy to use, everyday transactions, control you own coins
- Cons: Online is more vulnerable to attacks, you can make mistakes

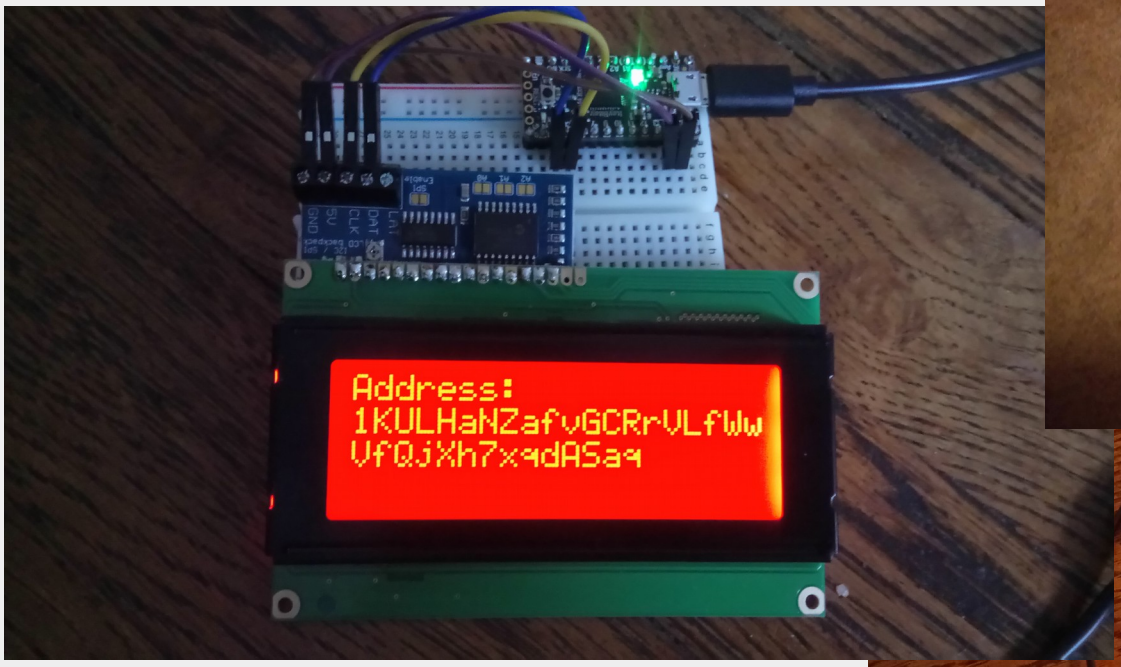
Offline Wallets

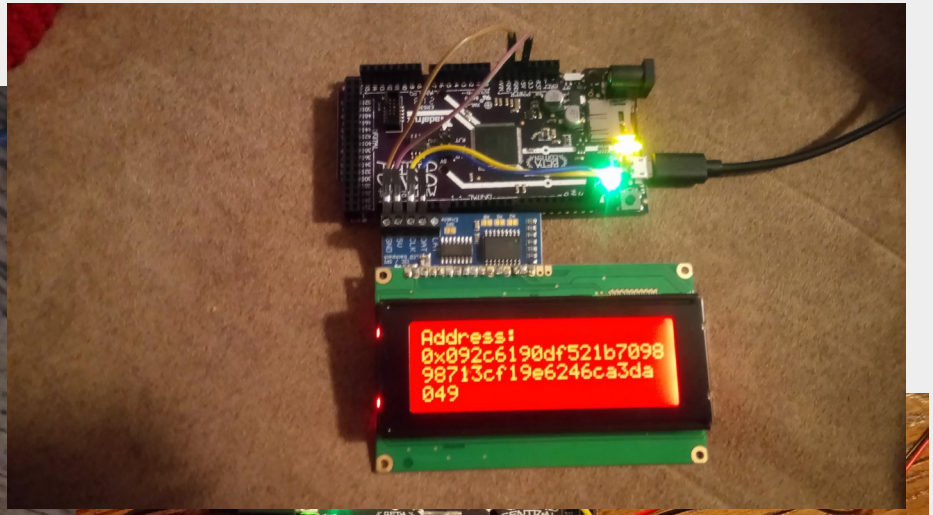
- Ex: KeepKey, Ledger, Paper wallets
- You control private keys, stored with no internet connection
- Pros: Highest level of security, long term storage
- Cons: Most complicated
  - Paper/metal wallets are easy to screw up
  - Hardware wallets less so – preferred method

Offline Wallets

If you’re extra nerdy, make your own!

https://github.com/chaintuts/ubitaddr/tree/development





Potential Threats

- Exchange goes under or steals your coins
  - Mt. Gox, Quadriga CX
- SIM swap attacks used to gain access
- DNS hijacking/malware swaps address
- Social engineering
- Physical attacks (the ol’ wrench attack)

So What Should I Use?

- Factors to consider: level of tech savvy, use cases, amounts
  - Custodial: Great for small amounts, purchase/sell, non-tech savvy
  - Online: For day to day purchases, small to medium amounts, reasonably savvy
  - Offline: Large amounts, long term savings, more tech savvy individuals (hardware wallets help bridge the gap)

Final Thoughts

- Remember, **private keys** are the core of our security focus
- ***Not your keys, not your Bitcoin!***
- Before you Bitcoin, know:
  - Your level of technical knowledge
  - Your threat model and usage (amounts, spend vs. save, etc.)
  - Understand core concepts and ask for help if you need it!

Questions?