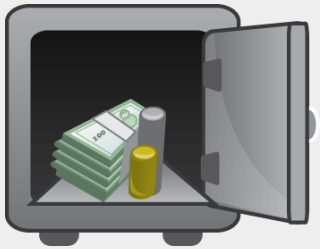
Cryptocurrency Security Fundamentals

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

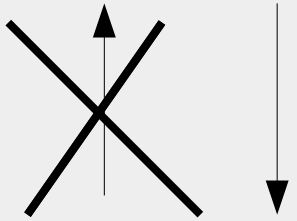
- Security is a *complex, evolving* topic
- There is not a one size fits all solution
- Know your threat model, and learn about tools you can use
- **We'll discuss some Bitcoin fundamentals and the surrounding security tools**



The Core of Crypto Ownership: Private Keys

0x12351bc143badf2348fe38e8f8b785b...

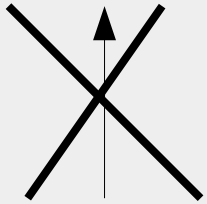
PRIVATE KEY



Elliptic Curve
(secp256k1)

0x04135981abcd7f7a7d7b7c720....

PUBLIC KEY



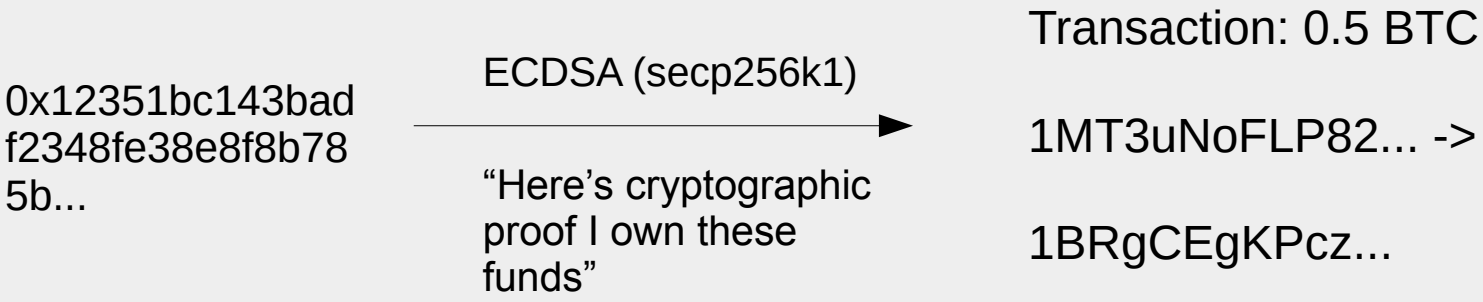
“Double hash” (SHA-256
and RIPEMD160)
And Base58check encoding

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

ADDRESS
(PUBLIC KEY
HASH)

The Core of Crypto Ownership: Private Keys

- Private keys are what we need to keep safe the most!
- Keys are never shared – only used to “sign” your transactions, proving you own funds



Private Keys & The #1 Rule...

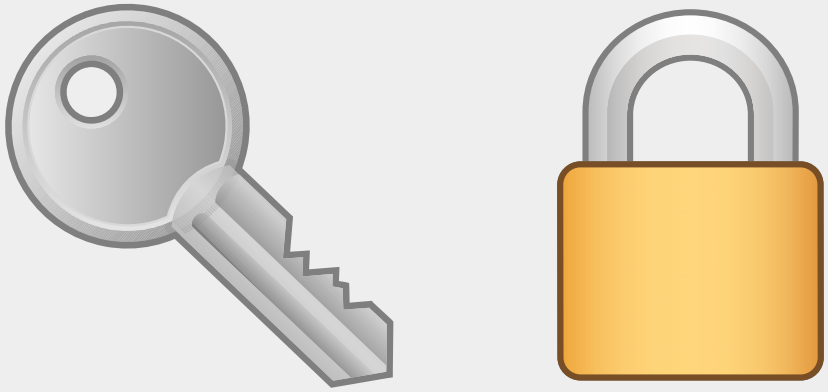
Not your keys…

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, other exchanges
- Keys are held for you by the wallet provider (you don’t have direct access to them)
- Similar to a traditional banking model

Custodial Wallets

- Pros:
  - Ease of use for beginners (no keys to lose)
  - Dedicated security pros managing private keys

Custodial Wallets

- Cons:
  - Rule #1 – Not your keys, ***Not your Bitcoin***
  - Vulnerable to traditional banking failures
    - Singular target for thieves
    - Insider theft
    - Censorship/Freezing your funds

Custodial Wallets

- Security Practices
  - Use *strong* 2FA – Authenticator app > SMS
  - Use a strong passphrase! - The longer the better, and NO reuse
  - Secure your *email* in the same way
  - Use only for purchases or storing small amounts for spending
  - In general, storing funds here is **not** recommended! The funds are ***not really yours!***

Online Wallets

- Ex: Mobile wallets (Bitcoin.com, Coinomi, etc.), Full Node PC wallets (Bitcoin ABC, Litecoin Core, etc.)
- Keys are generated and stored on an online device
  - Usually generated from a seed phrase these days
  - Could be randomly generated as well

Online Wallets

- Pros:
  - Generally still easy to use – more work/understanding than custodial solutions
  - Robust feature sets and security options (extra PIN, Encryption, etc.)
  - Funds are readily accessible for spending (online)

Online Wallets

- Cons:
  - Vulnerable to malware and “prying eyes” on the network
    - Ex: Electrum attack – users tricked into downloading malicious wallet
    - Could observe key generation/steal keys from disk
  - Require some knowledge to safely store and backup keys/seed phrases

Online Wallets

- Security Practices
  - Backup keys/seed phrases upon setup – offline if possible
  - Use wallet encryption, access/spending PIN, etc.
  - Only use for reasonable amounts that you'll be spending/using somewhat often
  - Suggested route for short/medium term use. Hold your own keys!

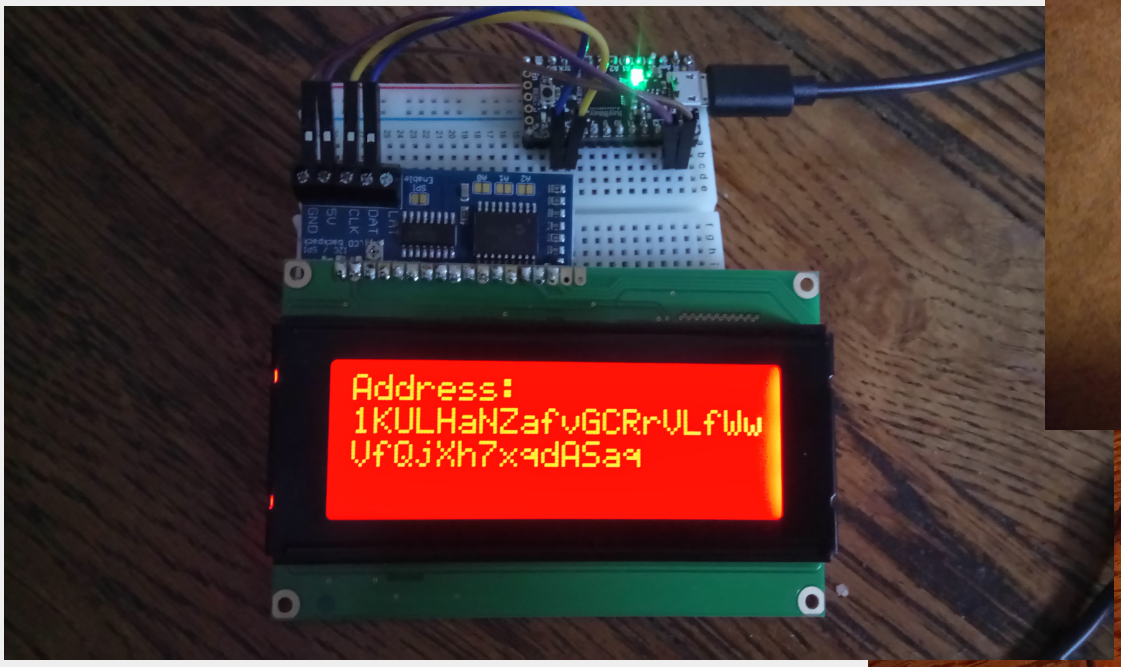
Offline Wallets

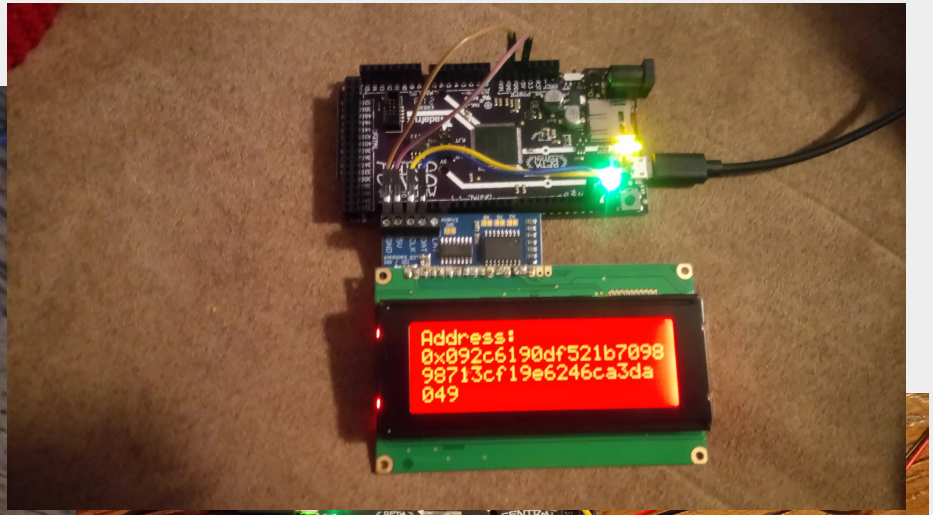
- Ex: Hardware Wallets (Keepkey, Trezor, etc.) and Paper/Metal/etc. Wallets
- Keys are generated and stored on a device not connected to a network
  - Could be from a seed phrase, or random
  - Generated on dedicated hardware, or an offline PC

Offline Wallets

If you’re extra nerdy, make your own!

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





Offline Wallets

- Pros:
  - Robust security – not vulnerable to network attacks
    - Keys have to be *physically* stolen
    - Key generation is difficult to observe
    - Can’t create/sign a malicious tx
  - Resistant to data loss from computing failures (phone in toilet, HDD failure, loss/theft from daily use)

Offline Wallets

- Cons:
  - Highest level of technical knowledge needed for safety
  - Can be vulnerable to environmental failures (fire, burglary, flooding)
  - Need to create copies (seed phrase, keys, etc.) in case of failure
  - Requires more work to spend funds later

Offline Wallets

- Security Practices
  - Create backups – multiple paper/metal/etc. Wallets, or backup seed phrases
  - Store in a physically safe location – safety deposit box, home safe, etc.
  - Understand risks before you use – UI is not as user friendly
  - Recommended for long term storage of savings

What We Didn’t Cover

- Privacy – that’s a whole ‘nother animal
  - Privacy concerns connecting you with your transactions (how much you have, what you purchase, etc.)
- Physical Bitcoin Attacks
  - Person-to-person coercion
  - See Lopp.net for documented attacks
- Bad software implementations
  - Cryptography foot guns, etc.

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?

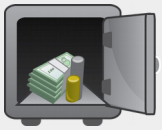
Cryptocurrency Security Fundamentals

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**



The Core of Crypto Ownership: Private Keys

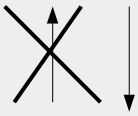
0x12351bc143badf2348fe38e8f8b785b...

PRIVATE KEY

Elliptic Curve
(secp256k1)

0x04135981abcd7f7a7d7b7c720….

PUBLIC KEY



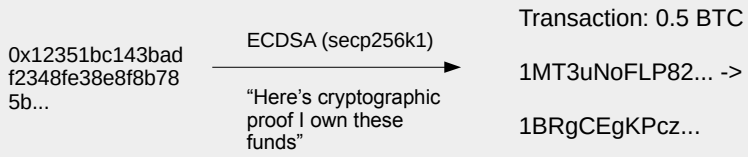
“Double hash” (SHA-256
and RIPEMD160)
And Base58check encoding

1MT3uNoFLP82j2aSD5Qtibm2kXJ7RWumAM

ADDRESS
(PUBLIC KEY
HASH)

The Core of Crypto Ownership: Private Keys

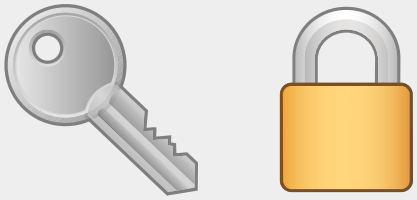
- Private keys are what we need to keep safe the most!
- Keys are never shared – only used to “sign” your transactions, proving you own funds



Private Keys & The #1 Rule...

Not your keys…

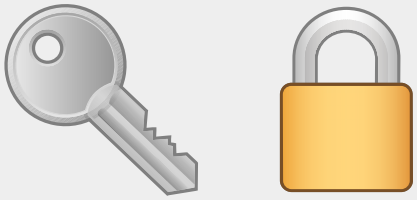
NOT YOUR BITCOIN



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, other exchanges
- Keys are held for you by the wallet provider (you don’t have direct access to them)
- Similar to a traditional banking model

Custodial Wallets

- Pros:
  - Ease of use for beginners (no keys to lose)
  - Dedicated security pros managing private keys

Custodial Wallets

- Cons:
  - Rule #1 – Not your keys, ***Not your Bitcoin***
  - Vulnerable to traditional banking failures
    - Singular target for thieves
    - Insider theft
    - Censorship/Freezing your funds

Custodial Wallets

- Security Practices
  - Use *strong* 2FA – Authenticator app > SMS
  - Use a strong passphrase! - The longer the better, and NO reuse
  - Secure your *email* in the same way
  - Use only for purchases or storing small amounts for spending
  - In general, storing funds here is **not** recommended! The funds are ***not really yours!***

Online Wallets

- Ex: Mobile wallets (Bitcoin.com, Coinomi, etc.), Full Node PC wallets (Bitcoin ABC, Litecoin Core, etc.)
- Keys are generated and stored on an online device
  - Usually generated from a seed phrase these days
  - Could be randomly generated as well

Online Wallets

- Pros:
  - Generally still easy to use – more work/understanding than custodial solutions
  - Robust feature sets and security options (extra PIN, Encryption, etc.)
  - Funds are readily accessible for spending (online)

Online Wallets

- Cons:
  - Vulnerable to malware and “prying eyes” on the network
    - Ex: Electrum attack – users tricked into downloading malicious wallet
    - Could observe key generation/steal keys from disk
  - Require some knowledge to safely store and backup keys/seed phrases

Online Wallets

- Security Practices
  - Backup keys/seed phrases upon setup – offline if possible
  - Use wallet encryption, access/spending PIN, etc.
  - Only use for reasonable amounts that you'll be spending/using somewhat often
  - Suggested route for short/medium term use. Hold your own keys!

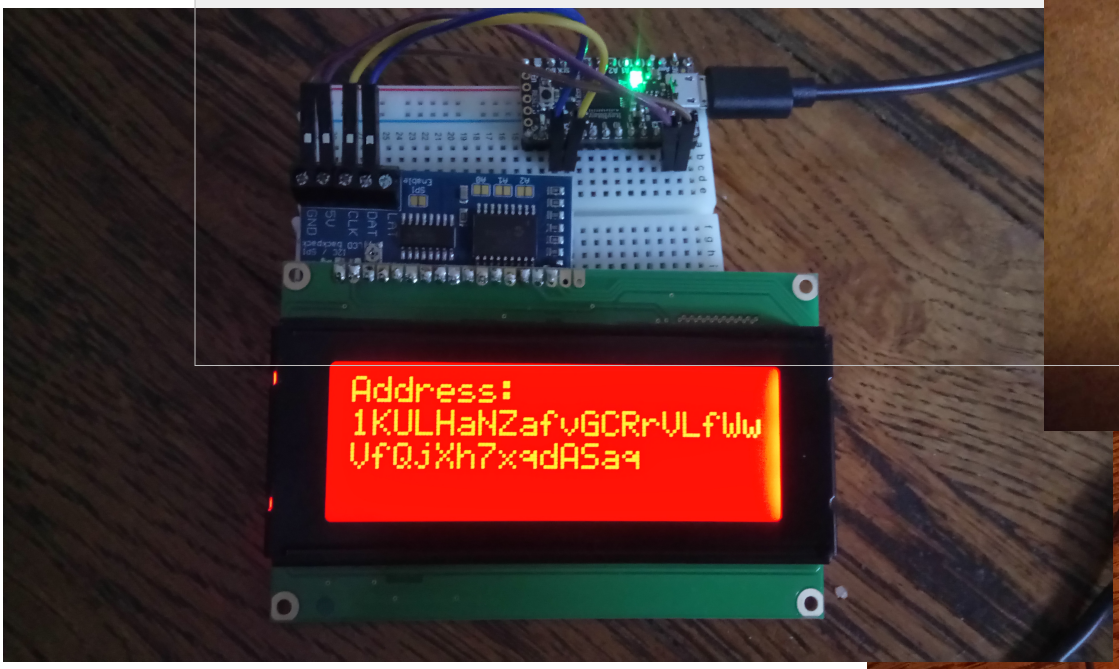
Offline Wallets

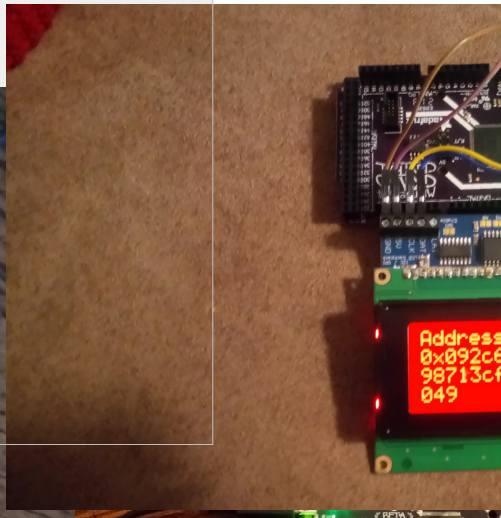
- Ex: Hardware Wallets (Keepkey, Trezor, etc.) and Paper/Metal/etc. Wallets
- Keys are generated and stored on a device not connected to a network
  - Could be from a seed phrase, or random
  - Generated on dedicated hardware, or an offline PC

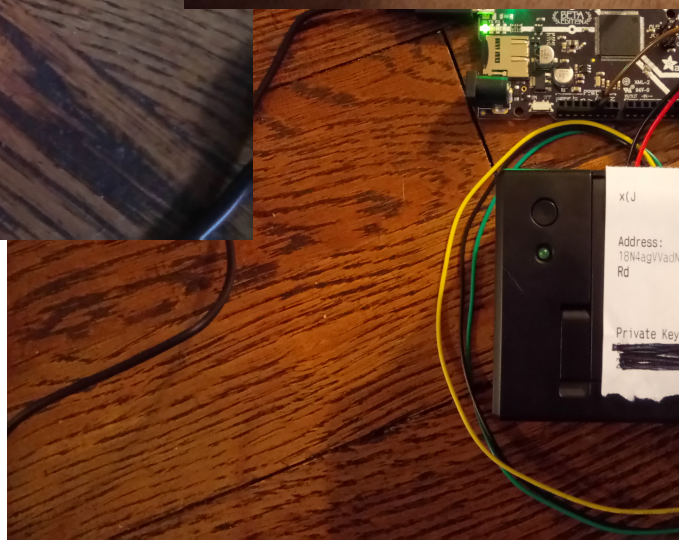
Offline Wallets

If you’re extra nerdy, make your own!

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







Offline Wallets

- Pros:
  - Robust security – not vulnerable to network attacks
    - Keys have to be *physically* stolen
    - Key generation is difficult to observe
    - Can’t create/sign a malicious tx
  - Resistant to data loss from computing failures (phone in toilet, HDD failure, loss/theft from daily use)

Offline Wallets

- Cons:
  - Highest level of technical knowledge needed for safety
  - Can be vulnerable to environmental failures (fire, burglary, flooding)
  - Need to create copies (seed phrase, keys, etc.) in case of failure
  - Requires more work to spend funds later

Offline Wallets

- Security Practices
  - Create backups – multiple paper/metal/etc. Wallets, or backup seed phrases
  - Store in a physically safe location – safety deposit box, home safe, etc.
  - Understand risks before you use – UI is not as user friendly
  - Recommended for long term storage of savings

What We Didn’t Cover

- Privacy – that’s a whole ‘nother animal
  - Privacy concerns connecting you with your transactions (how much you have, what you purchase, etc.)
- Physical Bitcoin Attacks
  - Person-to-person coercion
  - See Lopp.net for documented attacks
- Bad software implementations
  - Cryptography foot guns, etc.

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?