

CMPSC 390

Bitcoin Interactions

Janyl Jumadinova

February 1, 2021

Light Nodes (SPV Nodes)

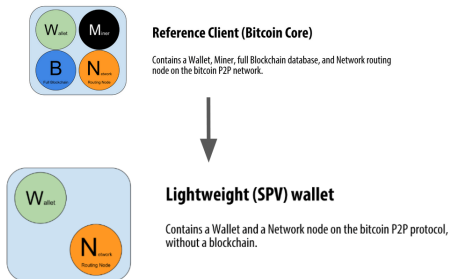
Simple Payment Verification (SPV):

a method for verifying if particular transactions are included in a block without downloading the entire block.

Light Nodes (SPV Nodes)

Simple Payment Verification (SPV):

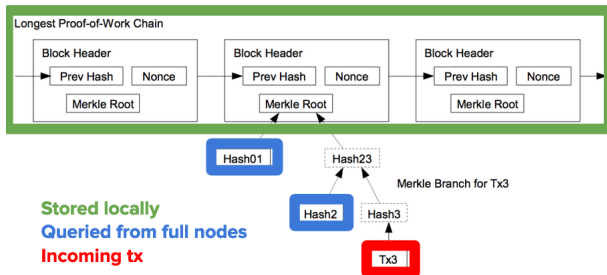
a method for verifying if particular transactions are included in a block without downloading the entire block.



Simple Payment Verification

Assumption:

Incoming block headers are not from a false chain.



Bitcoin Wallets

Bitcoin Wallets

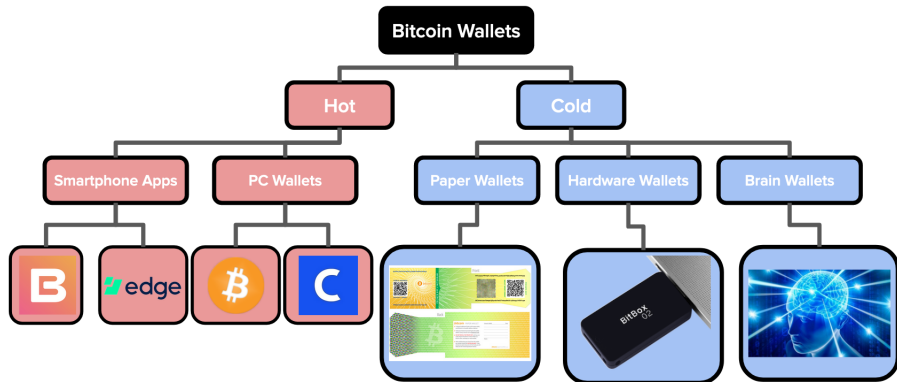
- Provides a user interface to the blockchain
- Keep track of the private key
- Store, send, receive, and list transactions
- Maybe some other functionalities

Bitcoin Wallets

- Provides a user interface to the blockchain
- Keep track of the private key
- Store, send, receive, and list transactions
- Maybe some other functionalities

<https://bitcoin.org/en/choose-your-wallet>

Types of Wallets



Creating a Wallet

- Paper/hardware wallet (example: <https://walletgenerator.net/>)
- Digital wallet (example: <https://login.blockchain.com/#/signup>)

Getting bitcoin

- Bitcoin ATMs (<https://coinucopia.io/>)

Getting bitcoin

- Bitcoin ATMs (<https://coinucopia.io/>)
- Centralized Exchanges (<https://bitcoin.org/en/exchanges>)

Getting bitcoin

- Bitcoin ATMs (<https://coinucopia.io/>)
- Centralized Exchanges (<https://bitcoin.org/en/exchanges>)
- Decentralized Exchanges (DEXs) (example: <https://bisq.network/>)

Best Practices

- Multisignature
- Never reuse pseudonyms, public keys
 - Wallet software can handle this

Hierarchical Deterministic (HD) Wallets

- Deterministic because all child keys are generated from a seed in the same way every time.
- **Hierarchical**: you can organize the keys in a tree-like structure, with levels.

