BLOCKCHAIN TECHNOLOGY

Bitcoin Network and Payments

The Bitcoin network

- a peer-to-peer network
  - where nodes exchange transactions and blocks.
  - two main types of nodes
    - full nodes
      - implementations of Bitcoin core clients
      - performing
        - Wallet
        - Miner
        - full blockchain storage
        - network routing functions.
    - Simple Payment Verification (SPV) nodes
      - Also called lightweight clients
      - perform only wallet and network routing functionality
      - Can function without a blockchain
        - only download the headers of the blocks
        - they can request transactions from full nodes

The Bitcoin network

- a peer-to-peer network
  - a few nonstandard but heavily used nodes
    - are called pool protocol servers
    - make use of alternative protocols
      - such as the stratum protocol.
        - a line-based protocol
        - makes use of TCP sockets and human-readable JSON-RPC
    - are used in mining pools.
    - Some nodes only compute hashes
      - use the stratum protocol to submit their solutions to the mining pool

The Bitcoin network

- a peer-to-peer network
  - There are 27 types of protocol messages
  - likely to increase over time as the protocol grows.
  - Most used protocol messages
    - version
      - the first message that a node sends out to the network
        - advertising its version and block count
      - The remote node then replies with the same information and the connection is then established.

The Bitcoin network

- a peer-to-peer network
  - Most used protocol messages
    - verack
      - the response of the version message accepting the connection request
    - inv
      - used by nodes to advertise their knowledge of blocks and transactions
    - getdata
      - response to inv, requesting a single block or transaction identified by its hash.

The Bitcoin network

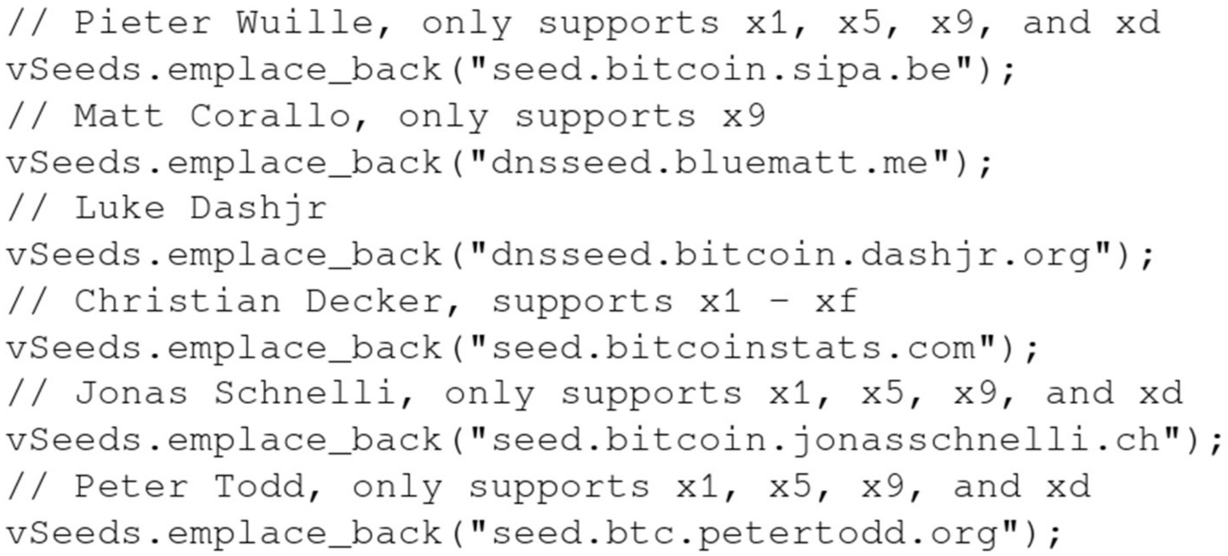
- a peer-to-peer network
  - Most used protocol messages
    - getblocks
      - returns an inv packet containing the list of all blocks starting after the last known hash or 500 blocks.
    - getheaders
      - is used to request block headers in a specified range
    - tx
      - is used to send a transaction as a response to the getdata
    - block
      - sends a block in response to the getdata

The Bitcoin network

- a peer-to-peer network
  - Most used protocol messages
    - headers
      - returns up to 2,000 block headers as a reply to the getheaders request
    - getaddr
      - is sent as a request to get information about known peers
    - addr
      - provides information about nodes on the network.
      - contains address list in the form of IP address and port number.

The Bitcoin network

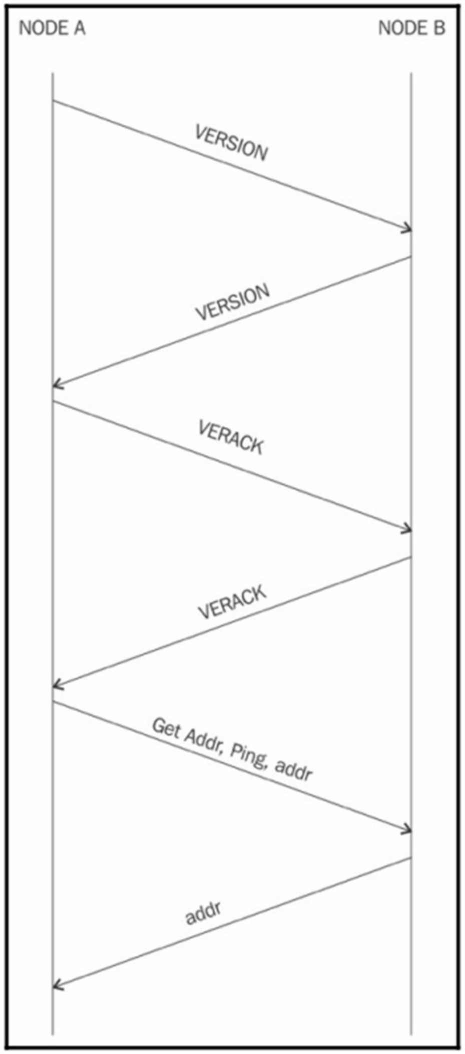
- When a Bitcoin core node starts up
  - it initiates the discovery of all peers
    - achieved by querying DNS seeds
      - hardcoded into the Bitcoin core client
      - maintained by Bitcoin community members



```
// Pieter Wuille, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.bitcoin.sipa.be");
// Matt Corallo, only supports x9
vSeeds.emplace_back("dnsseed.bluematt.me");
// Luke Dashjr
vSeeds.emplace_back("dnsseed.bitcoin.dashjr.org");
// Christian Decker, supports x1 - xf
vSeeds.emplace_back("seed.bitcoinstats.com");
// Jonas Schnelli, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.bitcoin.jonasschnelli.ch");
// Peter Todd, only supports x1, x5, x9, and xd
vSeeds.emplace_back("seed.btc.petertodd.org");
```

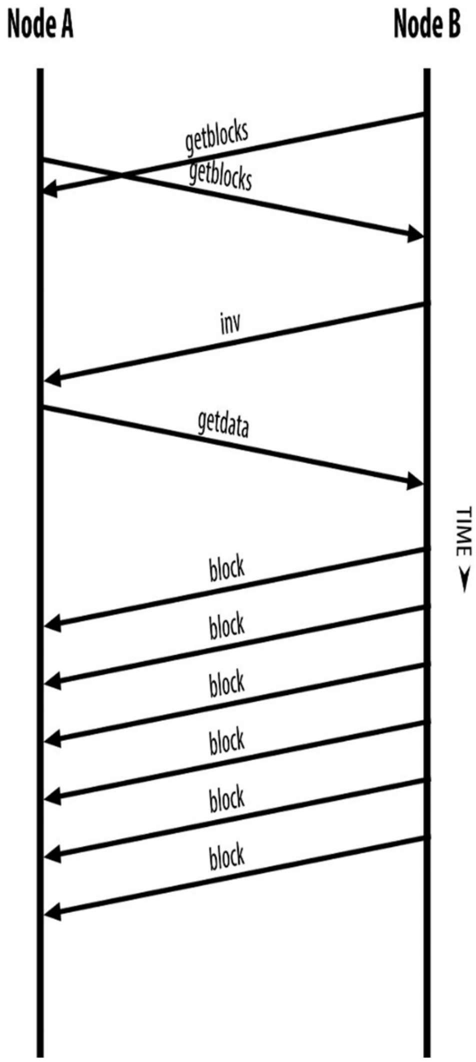
The Bitcoin network

- NODE A starts the connection
  - by sending the version message
    - contains BestHeight, a node's current number of blocks
- NODE B then responds with its own version message
- NODE A and NODE B then exchange a verack message
  - indicating that the connection has been successfully established.
- Then the peers can exchange getaddr and addr messages
  - to discover other peers on the network



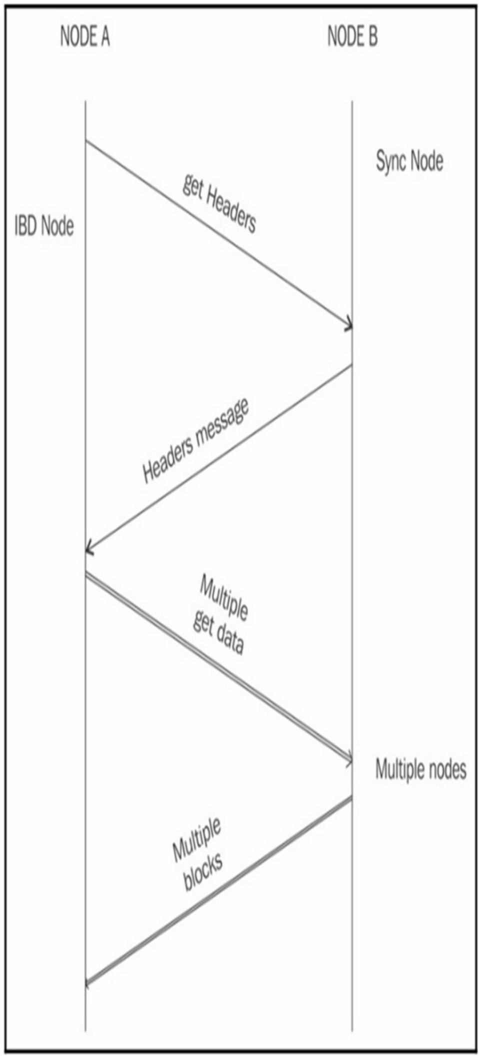
The Bitcoin network

- Peered nodes will exchange a getblocks message
  - contains the hash of the top block on their local blockchain.
- The peer that has the longer chain
  - identify the first 500 blocks
  - transmit their hashes using an inv message.
- The node missing the blocks
  - retrieve them, by issuing a series of getdata messages
  - using the hashes from the inv message.



The Bitcoin network

- headers-first approach
  - Previous method was called blocks-first approach
    - Was very slow
  - Replaced with headers-first approach
    - resulted in major performance improvement
    - new node first gets block headers and validates them
    - Next, blocks are requested in parallel from all available peers



Wallets

- wallet software is used to
  - store private or public keys and Bitcoin address.
  - as receiving and sending bitcoins (Bitcoin client)
  - different types
    - Non-deterministic wallets
    - Deterministic wallets
    - Hierarchical Deterministic wallets
    - Brain wallets
    - Paper wallets
    - Hardware wallets
    - Online wallets
    - Mobile wallets

Wallets

- Non-deterministic wallets
  - contain randomly generated private keys
  - are also called just a bunch of key wallets.
  - Managing keys is very difficult and an error-prone
    - can lead to theft and loss of coins
    - there is a need to create regular backups

Wallets

- Deterministic wallets
  - keys are derived out of a seed value via hash functions.
  - This seed number
    - is generated randomly
    - is commonly represented by human-readable mnemonic code words.
  - Mnemonic code words can be used to recover all keys
    - makes private key management comparatively easier

Wallets

- Hierarchical Deterministic wallets (HD)
  - store keys in a tree structure derived from a seed
  - The seed generates the parent key (master key)
  - Master key is used to generate child keys and, subsequently, grandchild keys.
  - does not generate keys directly
    - it produces some information (private key generation information)
      - can be used to generate a sequence of private keys.
  - The complete hierarchy is easily recoverable
    - if the master private key is known.
  - are very easy to maintain and are highly portable

Wallets

- Brain wallets
  - master private key can also be derived from the hash of passwords that are memorized.
  - Can result in a full HD wallet that is derived from a single memorized password.
  - is prone to
    - password guessing
    - brute force attacks

Wallets

- Paper wallets
  - a paper-based wallet with the required key material printed on it.
  - It requires physical security to be stored
- Hardware wallets
  - a tamper-resistant device to store keys
  - can be
    - custom-built
    - A Secure Element (SE) in NFC phones

Wallets

- Online wallets
  - Are stored entirely online
  - are provided as a service usually via the cloud.
  - provide a web interface to the users to
    - manage their wallets
    - perform various functions such as making and receiving payments
  - They are easy to use
    - but imply that the user trusts the online wallet service provider

Wallets

- Mobile wallets
  - are installed on mobile devices
  - can provide various methods to make payments
    - most notably scaninng QR codes quickly and make payments

Wallets

- Wallet choice depends on factors such as
  - Security
  - ease of use
  - available features. Out of all these attributes,
- security should be of paramount importance
  - Hardware wallets tend to be more secure
  - Web wallets are not as secure as a hardware device.
- mobile wallets are quite popular
  - due to a balanced combination of features and security.

Bitcoin Improvement Proposals (BIPs)

- are used to propose or inform the Bitcoin community about
  - The improvements suggested
  - the design issues
  - or information about some aspects of the bitcoin ecosystem.
- three types of Bitcoin improvement proposals:
  - Standard BIP
    - Used to describe the major changes that have a major impact on the Bitcoin system
      - E.g., block size changes, network protocol changes, or transaction verification changes.
  - Process BIP
    - usually deal with proposing a change in a process that is outside the core Bitcoin protocol.
    - are implemented only after a consensus among bitcoin users.
  - Informational BIP
    - are usually used to record some information about the Bitcoin
    - E.g., design issues.

Advanced protocols

- Transaction throughput is a critical issues
  - Bitcoin network can only process about 3 to 7 tps
  - Visa can process about 24,000 tps
  - PayPal can process about 200 tps
  - Ethereum can process up to on average 20 tps.

Advanced protocols

- Segregated Witness (SegWit)
  - a soft fork to the Bitcoin protocol
  - addresses some weaknesses such as throughput and security
  - Reorganizes the block data
    - results in reduced size of the transaction
    - More transaction per block

Advanced protocols

- Bitcoin Cash
  - increases the block limit to 8 MB
  - uses PoW as consensus algorithm
    - Mining hardware is still ASIC based.
  - The block interval is changed from 10 minutes to 10 seconds and up to 2 hours.

Advanced protocols

- Bitcoin Unlimited
  - block size is increased
    - but not set to a hard limit.
  - Miners come to a consensus on the block size cap over a period.
  - Other concepts
    - parallel validation
      - allows nodes to validate more than one block in parallel
      - When a node receives a block in bitcoin
        - Should validate it
        - Then accept it or reject it
        - cannot relay new transactions or validate any blocks during validation period
    - extreme thin blocks
      - fixes an inefficiency in Bitcoin
        - transaction are regularly received twice
          - once at the time of broadcast by the sender
          - then again when a mined block is broadcasted

Advanced protocols

- Bitcoin Gold
    - a hard fork since of the original Bitcoin blockchain. resulted in a new blockchain, named Bitcoin Gold (BTG)
    - The core idea is to address the issue of mining centralization
        - power shifts towards miners with more hashing power
        - Uses the Equihash mining algorithm
            - is inherently ASIC resistant
            - uses GPUs for mining