The Bitcoin P2P Protocol

Ryan X. Charles
Blockchain University
Tokyo, Dec. 19, 2015

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Outline

- Basic message data structure
- Commands:
  - block, getblocks, getdata, getheaders, headers, inv, mempool, merkleblock, notfound, tx, addr, alert, filteradd, filterclear, getaddr, ping, pong, reject, verack
- The future of P2P: web sockets & Web RTC

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

The Basics

- Bitcoin “full nodes” connect to each other over tcp
- Send bitcoin-specific “message” data structures back and forth
- Not all nodes are full nodes. Light nodes, or SPV nodes, also connect to the network, but do not download entire blockchain
- Pruning nodes exist, that download but do not permanently store blockchain

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Message Structure

- [magicnum][cmd][datasize][checksum][data]
- magicnum: constant 32 bit unsigned int
- cmd: 12 byte string (“inv”, “getblock”, etc.)
- datasize: 32 bit unsigned int
- checksum: first 4 bytes of sha256sha256(data)
- data: any number of bytes representing the data of the message

Inventory

- A data structure used to communicate certain types of data, particularly txs and blocks.
- [type][hash]
- Types:
  - MSG_TX: hash is a tx hash
  - MSG_BLOCK: hash is a block hash
  - MSG_FILTEREDBLOCK: “merkle” block for SPV wallets

Block

- cmd: “block”
- data: [block]
- Usually sent in response to a request for a particular block
- Can also be broadcast unrequested

Get Blocks

- cmd: “getblocks”
- data: [version][hashcount][hashes][stophash]
- Sender sends a list of blocks they have (or rather, the hashes of those blocks), and the responder will send back an “inv” containing blocks they have near the blocks of the requester

Get Data

- cmd: “getdata”
- data: [numinvs][inventories]
- Sender requests particular pieces of data, e.g. transactions, blocks, or merkle blocks

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Get Headers

- cmd: “getheaders”
- data: [version][hashcount][hashes][stophash]
- Sender requests block hashes, with the intent of downloading headers only. Only difference from “getblocks” is that the responder will send as many as 2000 block ids rather than 500

Headers

- cmd: “headers”
- data: [numheaders][headers]
- Send a list of block headers. Useful for “headers-first” blockchain download or SPV clients.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Inventory

- cmd: “inv”
- data: [numinvs][inventories]
- Send inventory, i.e. what transactions or blocks this node has, so the receiver can pick among them to download. Can be sent unsolicited to announce new blocks, or in response to getblocks or mempool.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Mempool

- cmd: “mempool”
- data: blank
- The sender wants to find out what transactions are in the mempool of the receiver and are not yet in a block. The responder sends an inventory of such transactions.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Merkleblock

- cmd: “merkleblock”
- data: [blockheader][txcount][hashcount][hashes][flagcount][flags]
- A reply to a getdata where the requester wants a merkleblock.
- blockheader: The block header.
- txcount: How many transactions are in the block
- hashcount: how many hashes match filter
- hashes: list of hashes
- flagbytecount: how many flags
- flagbytes: a series of bytes where each bit represents the position of the tx in the merkle tree, e.g. 0101100

Notfound

- cmd: “notfound”
- data: [numinvs][inventories]
- In response to a getdata message, tell the node which pieces of data (transactions, blocks or merkle blocks) were not found.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Tx

- cmd: “tx”
- data: [tx]
- Can be sent in response to a getdata command. Can also be sent unsolicited, e.g. for broadcasting a new transaction. Might send many in sequence.

Addr

- cmd: “addr”
- data: [numaddrs][addrs]
- addr: [time][services][ip][port]
- A way for nodes to send their connection information and connection of other peers, so that each peer can easily find other peers on the network by listening for these messages.

Alert

- cmd: “alert”
- data: [alertlen][alert][siglen][sig]
- If there is some reason for the Bitcoin Core developers to send an “alert”, e.g. if there is an unintentional blockchain fork in progress, they can send a signed alert. Only some Core developers have the private key to send an alert.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Filter Add

- cmd: “filteradd”
- data: [elementlen][element]
- Tells the node to add an element to an existing Bloom filter. Each element is a filter of up to 520 bytes long (the max size of a script). Matches against various parts of a transaction, including elements pushed to the stack, which includes addresses.

Filter Clear

- cmd: “filterclear”
- data: blank
- Clear the filter set on that node.

Filter Load

- cmd: “filterload”
- data: [nfilterbytes][filter][nhashfuncs][ntweak][nflags]
- Load a new Bloom filter so that the receiver knows how to filter all transactions and merkleblocks being relayed to this node.
- nfilterbytes: number of bytes in filter, varint.
- filter: up to 520 bytes of data
- nhashfuncs: number of hash functions to perform, uint 32.
- ntweak: arbitrary value to add to seed for hashing, uint 32.
- nflags: flags to control how filters are matched, uint 8.

Get Addr

- cmd: “getaddr”
- data: blank
- Request an addr message that contains a big list of nodes to connect to.

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt

Ping

- cmd: “ping”
- data: [nonce]
- Request a pong message. Helps to debug bitcoin p2p network connections. Nonce is 8 bytes of usually random data.

Pong

- cmd: “pong”
- data: [nonce]
- Send a pong message in response to a ping. The nonce should be the same as in the ping.

Reject

- cmd: “reject”
- data: [messagelen][message][code][reasonlen][reason][extradata]
- Informs a node that one of its previous messages was rejected for some reason. Very helpful for debugging.

VerAck

- cmd: “verack”
- data: blank
- Acknowledges a previously received version message.

Version

- cmd: “version”
- data: [version][services][timestamp][addr_recv services][addr_recv IP address][addr_recv port][addr_trans services][addr_trans IP address][addr_trans port][nonce][user_agent bytes][user_agent][start_height][relay]
- Sent at the start of a connection to inform the other node what version of the p2p protocol is being used.
- start_height: height of perceived blockchain
- relay: whether this node wants to relay txs

Future of P2P

- P2P works only over TCP
- Web can use:
  - Web sockets – good for browser ↔ server
  - Web RTC – good for browser ↔ browser
- See: fullnode, bitcore, webcoin, bcoin

Ryan X. Charles
Founder of Datt (datt.co)
twitter.com/ryanxcharles
github.com/ryanxcharles

Code Samples and Slides at:
github.com/ryanxcharles/blockchain-university

Datt