Buy/Sell order format:

* Fee tx
  + Raw tx + path to merkle root
  + Fixed at $11 worth of coins at time of payment
  + Contains a hash of the list of areas that the offer is valid in + the market + the public key + order type + fiat currency + cryptocurrency
  + Used to mitigate spam (make it expensive to spam offers)
  + Also used to fund development!
* Order type (buy/sell)
  + Locked into fee tx
* Max AMT
  + Measured in coins if sell order and fiat if buy order
  + Should/can be adjusted as people take small parts of your offer bit by bit
* Min AMT
  + Measured in coins if sell order and fiat if buy order
* Price
  + Relative to last price (not fixed)
  + Locked into fee tx
* Fiat currency
  + Locked into fee tx
  + Can be any out of large list
  + All fiat currencies are valid in all shards (locations)
* Cryptocurrency
  + Locked into fee tx
  + Must be Bitcoin (for MVP)
* Valid areas (max 4)
  + List if shard IDs where this offer is valid
  + Locked into fee tx
* Approx coordinates (very approximate)
  + Can be changed by user over the course of the trade depending on the location of the seller
* Public key of sender
  + Locked into fee tx
  + Used to prevent maleating of offer by relaying nodes
  + And to prevent fee tx from being used by other people
* Sequence number
  + Incremented every time offer is edited so nodes know which version is newer
  + Limited to 15 edits periffer to prevent spam edits since they get flooded in network (it has a max value of 15)
* Description
  + Might include trade details
  + Available times
  + Requirements
  + max/min amounts
  + Links to other profiles
* Contact method
  + Such as phone, signal, wire, telegram, ricochet
  + Used for organising trade location, time and details between parties
* Timeout
  + Counted since fee tx date
  + Must be smaller than max timeout length (~14 days)
  + Actually can be as big as needed but will be maxed out
* Signature
  + (from priv key of first address in fee tx) of all fields in offer to prevent malleability and prove ownership of fee tx

P2P network message types:

* Change offer
* Create offer
* Delete offer
  + Is really just a change offer command that sets the timeout time to zero

General information:

* Violations of any protocol standards leads to a temporary (few weeks) block
  + This dis-incentivises nodes from relaying or creating spam
  + Able to be circumvented by changing node ip address
* The network is split into partitions based on location
  + Each shard, its size and its coordinates is deterministic and can be calculated by all nodes
  + All shards are the same size
  + Nodes can be a part of multiple shards if they want to
* Fee txs contain hash or beginning of hash of all fields (in op\_return) in the offer that are "locked" and can't be changed while using the same fee tx
  + This could actually be the merkle root instead
* Messages are flooded through the entire shard (only one shard)
  + Each node will only relay max (~50) messages per offer and every message includes proof of offer tx + public key of receiver for deletion purposes
  + Messages are only valid on shards that are listed in the locations field that is committed in the fee tx by its hash (or merkle root)
  + Nodes might limit the amount of messages per offer according to the size of the fee paid
* Proof of fund tx
  + Used to mitigate spam (require that you actually have the necessary funds to make your tx)
  + Not possible with buy orders since you can't prove ownership of fiat
  + Contains raw tx that spends the => the offered amount of crypto to an output
  + Merkle path to block
  + Contains list of locations in which it can be used (max (4))
  + Next to the tx in the offer is a signature from one of the output addresses of the tx to prove ownership, and it is will sign the other sections of the offer
  + Txid
    - The reason for inclusion of a txid is that since this tx is spendable, the funds could be spent somewhere else and so therefore each node needs to check that the tx value output is unspent by asking a full node for a proof of spend and this requires knowledge of the txid+output index (so tye txid is provided here to speed up the process.
* Account age via bch blockchain commitment
* Ability to add "contacts" or trusted users based on their public key
* Fee should be fixed per offer as increased offer value does not create spam but instead increased offer count creates spam
* Password protection
* Export wallet
* Tor integration
* Pay more fees for a longer timeout time (up to a limit)
* Support monero + bitcoin cash eventually
* username reserved by putting it into block and then nodes see which one was earlier
* Commit locked fields to fee tx using merkle root
* Network sharding by market
* <https://medium.com/perlin-network/noise-an-opinionated-p2p-networking-stack-for-decentralized-protocols-in-go-bfc6fecf157d>
* Dynamic shard sizing
* Kademlia routing algo for dht network
* <https://gitlab.com/kadence/kadence> seems like a good node.js dht lib
* Use Kademlia instead of flood network
* Compress offers for bandwidth

Minimal Viable Product Details

* Nodes use external messaging services (i.e. Telegram)
* No account age record
* Nodes block other nodes for miss-behaviour
* Network is sharded by geography and not by market
* All accounts are anonymous and have no "username"
* Fee is fixed at ~USD$11 calculated from current exchange rate from exchange API
* Nodes validate the fee is the correct value based on bitcoin price at time of fee tx with some leniency by keeping a local record of historical prices
* Proof of funds is not required on sell orders
* All orders have a timeout and a default max timeout calculated from date of fee tx
* Bitcoin is only coin supported
* Fee tx contains hash of locked in fields
* Can delete offers by editing them to make their timeout date < current time
* Can edit "non-locked in" order fields
* Buy and sell orders both require fee
* Clearnet only, not hidden services
* Will ban peers that misbehave - this might not work if lots of phones share the same 4g ip in the same area as they often do
* Will connect to ~10 peers
* Nodes keep cache since maxTimeout days ago of Bitcoin price at 1 hour intervals for fee tx any validation without needing to connect to server
* Not password protected
* Locked in offer fields are (ones hashed into fee tx:
  + Public key
  + Valid shard ids
  + Fiat currency
  + Cryptocurrencies
  + Order type
* All fiat currencies are valid in all shards
* Nodes validate each offer's attributes in the following order for efficiency purposes:
  + Must be smaller than 2kb
  + If already have offer with the same hash
  + Fee tx is valid
  + If fee tx is not older than max age
  + All necessary fields exist
  + Locked in fields match commitment in fee tx
  + In valid shard
  + Timeout = max(timeoutField, maxTimeout)
  + Not timed out yet (based on timeout field)
  + No more than four shards specified
  + Signature is valid
  + Fiat currency is valid (in a list)
  + Cryptocurrency is Bitcoin (for MVP)
  + If sequence number is less than 15
  + If sequence number is > than current stored version
  + If already have offer with the same fee tx but different lower sequence number:
    - Replace with this offer
  + Elif True:
    - Save and re-broadcast to neighbours
* Will contain spv client for tx validation that selects full nodes from network (not like electrum)

Variables:

* Fee per offer: USD$11
* Max offer size: 2kb
* Max edit count (max sequence number): 20
* Size of shard:
* Max age of offer: 20 days
* Max shard count per offer: 4
* List of fiat currencies
* Amount of peers to connect to: 10

-----------------------------------

Node Methods